

N° d'enregistrement
au C.N.R.S.

THESE DE DOCTORAT D'ETAT ES SCIENCES MATHÉMATIQUES

présentée

A LA FACULTE DES SCIENCES
de PARIS

par

PIERRE LECOINTE

pour obtenir

le grade de Docteur Es-Sciences

Sujet de la Thèse: Etude Géométrique Des Plans D'Expériences Et Des Codes
Correcteurs D'Erreurs.

soutenue le

1970

devant la commission d'examen:

MM. DUGUE Président

BENZECRI Examineurs

ARIBAUD "

N° d'enregistrement

au C.N.R.S.

THESE DE DOCTORAT D'ETAT ES SCIENCES MATHÉMATIQUES

présentée

A LA FACULTE DES SCIENCES

de PARIS

par

PIERRE LECOINTE

pour obtenir

le grade de Docteur Es-Sciences

Sujet de la Thèse: Etude Géométrique Des Plans D'Expériences Et Des Codes
Correcteurs D'Erreurs.

soutenue le

devant la commission d'examen:

MM. DUGUE Président

BENZECRI Examineurs

ARIBAUD

"



THESE DE DOCTORAT D'ETAT ES SCIENCES MATHÉMATIQUES

présentée par M. Pierre Lécointe

ERRATA

Page 20 ligne 13: au lieu de: $j=1,2,\dots,\min(h,k)$

lire : $j=1,2,\dots,h$.

Page 168 ligne 6 : au lieu de: k points de $v : x_1, x_2, \dots, x_k$, le point de v suivant:

lire : k points de $v: x_1, x_2, \dots, x_k$ définissant v (c'est-à-dire que l'on peut en extraire h points qui soient indépendants), le point de v suivant:

INTRODUCTION

Il y a de nombreuses similitudes qui apparaissent entre le problème de la construction des codes correcteurs d'erreurs et celui de la construction des plans d'expériences et les mathématiciens n'ont pas été sans les remarquer.

On se propose dans ce travail d'essayer de réunir ces deux problèmes dans une même étude géométrique.

Dans le chapitre I, on expose en premier lieu une généralisation de la notion de réseaux géométriques (R).

La Théorie des réseaux n'avait été développée et utilisée jusqu'ici que dans le cas plan par Bruck, Ostrom et Guérin.

Elle est ici étendue au cas d'un espace de dimension k positive quelconque.

Après avoir dégagé les principales propriétés des réseaux (R), on définit les "arrangements (T_k) " et les "arrangements (T_k) orthogonaux" ; on fait alors correspondre à certaines classes de réseaux, les réseaux $(\hat{R})$, des familles d'arrangements (T_k) . On distingue enfin une classe de réseaux particulière, les réseaux $(R)_{k-1}$ à laquelle on associe une famille d'arrangements (T_k) orthogonaux, ceci en vue de l'étude des tableaux orthogonaux d'indice $\lambda = 1$.

Le sujet du chapitre I est justifié au chapitre suivant dans lequel on décrit les applications des réseaux géométriques et des arrangements (T_k) à la construction des codes correcteurs d'erreurs et des plans d'expériences.

Les principaux résultats dégagés sont les suivants :
- à un réseau $(\hat{R})_{h+k-t-1}$, correspond un code $(h+k, k)$ possédant la propriété P_{t+1} .

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41551504_0006

- à un réseau $(R)_{k-1}$ correspond un tableau orthogonal d'indice $\lambda = 1$.

On peut dès maintenant remarquer que le langage des réseaux géométriques permet d'étudier la théorie des codes correcteurs d'erreurs dans sa quasi-totalité mais qu'il n'en est pas de même pour les plans d'expériences.

Les seuls plans d'expériences dont les réseaux peuvent permettre l'étude sont les tableaux orthogonaux d'indice $\lambda = 1$, les carrés latins orthogonaux et leur généralisation, certains plans en blocs équilibrés ou partiellement équilibrés mais certainement pas tous.

On termine le chapitre II en montrant l'équivalence qui existe entre le problème de la construction des ovales généralisés et celui de la construction des réseaux $(R)_{k-1}$ complets.

Le chapitre III est presque entièrement consacré à une étude systématique des arrangements (T_k) orthogonaux. Les principales notions étudiées sont celles qui correspondent au produit direct, aux transversales, à l'idempotence et à l'isotopie dans l'étude des quasi-groupes. Aussi avons-nous usé de la même terminologie.

On donne ensuite quelques exemples de construction de réseaux : certains sont simples et ont déjà été signalés par Bose dans l'étude des tableaux orthogonaux.

Si on les a rappelés, c'est à titre d'illustration, notre langage étant sensiblement différent de celui de Monsieur Bose.

Dans le chapitre IV, on introduit une nouvelle classe de réseaux, les "réseaux cycliques" en vue d'étudier plus spécialement les codes cycliques.

On se borne ensuite dans les calculs au cas où l'ensemble de base X (alphabet du Code) peut être muni d'une structure de Corps de Galois.

Les deux chapitres suivants ont été repoussés dans une Annexe : ils constituent deux possibilités d'étude des mêmes problèmes que précédemment mais dans des optiques différentes.

Aussi, on a pensé qu'il était nécessaire de les dégager de l'ensemble du travail.

Dans la première partie de cette annexe, le chapitre V, on généralise la théorie des "Systèmes de Droites" décrite par Monsieur Bose et utilisée par Monsieur Guérin. On définit des "Systèmes de Plans" dans des espaces de dimension k positive quelconque mais finie.

Le résultat final est le suivant : moyennant une propriété appelée "Propriété (P)", on peut, à partir d'un système de Plans, construire des arrangements (T_k) orthogonaux.

Dans la deuxième partie, le chapitre VI, on s'intéresse aux structures de Treillis que l'on peut faire correspondre aux réseaux géométriques et aux systèmes de plans. Les seuls treillis simples à construire sont ceux que l'on associe aux systèmes de plans.

Mais cela ne nous permet pas pour autant d'en déduire l'existence d'arrangements (T_k) orthogonaux, la propriété (P) énoncée au chapitre IV n'étant pas automatiquement vérifiée.

Je remercie Monsieur le Professeur Dugué de bien avoir voulu assurer la direction de mon travail et d'avoir accepté de présider le Jury de cette thèse.

Je remercie Monsieur le Professeur Benzecri d'avoir accepté de faire partie du Jury.

Je remercie enfin Monsieur le Professeur Aribaud de tous ses conseils et de tous les rectificatifs qu'il a apportés à la rédaction de mon travail qui, sans lui, aurait été bien imparfaite.

C H A P I T R E I

Généralisation de la Notion de Réseaux Géométriques.

L'étude des réseaux et des familles de quasi-groupes que l'on peut leur associer a été introduite en mathématiques dans la construction d'ensembles de carrés latins orthogonaux. Les réseaux qui ont alors été définis étaient plans et prolongeables dans certains cas en une géométrie plane Euclidienne (références [1] , [2] et [3]) : il leur correspondait alors un ensemble complet de quasi-groupes mutuellement orthogonaux.

C'est cette notion que nous allons généraliser ici pour lui associer des familles d'arrangements (T_k) dont nous donnerons un procédé de construction en utilisant des structures de quasi-groupes.

I. Définition des réseaux (R).

1) - Définition des réseaux (R).

- Soient E et F deux ensembles finis d'éléments.
- Soit F_i , $i \in [1, N]$, une partition de F en N classes F_i avec $\text{Card } [F_i] \geq 2$.
- Soit R un sous-ensemble de $E \times F$.
- Soient q et k deux nombres entiers positifs avec $2 \leq k < N$

Le système $(E, F, \{F_i\}_{i \in [1, N]}, R, q, k)$ définit un réseau (R) de dimension k si les propriétés suivantes sont vérifiées :

- a) $\forall x \in E, \forall i \in [1, N]$, $\text{Card } [y : y \in F_i, (x, y) \in R] = 1$
 c'est-à-dire
 Pour tout élément x de E et pour tout $i \in [1, N]$, il existe un élément y de F_i et un seul tel que $(x, y_i) \in R$
- b) $\forall y \in F_i, \forall z \in F_j, i \neq j, (i, j) \in [1, N]^2$:

$$\text{Card} [x : x \in E, (x, y) \in R, (x, z) \in R] = q^{k-2}$$

c'est-à-dire

Pour tout couple (y, z) d'éléments de F appartenant respectivement à deux classes F_i et F_j quelconques mais différentes, il y a exactement q^{k-2} éléments x de E tels que :

$$(x, y) \in R \text{ et } (x, z) \in R.$$

$$c) \forall h > 2, \forall (i_1, i_2, \dots, i_h) \in [1, N]^h, i_1 \neq i_2 \neq \dots \neq i_h$$

$$\forall (y^1, y^2, \dots, y^h) \in F_{i_1} \times F_{i_2} \times \dots \times F_{i_h} :$$

$$\text{Card} [x : x \in E, (x, y^1) \in R, (x, y^2) \in R, \dots, (x, y^h) \in R] =$$

$$- \text{Soit } q^{k-2}, \text{ soit } q^{k-3}, \dots, \text{ soit } q^{k-h}, \text{ soit } 0, \text{ si } k \geq h$$

$$- \text{Soit } q^{k-2}, \text{ soit } q^{k-3}, \dots, \text{ soit } 1, \text{ soit } 0, \text{ si } k < h$$

c'est-à-dire

Pour tout entier $h > 2$ et pour tout ensemble de h éléments de F , $y^1, y^2, \dots, y^h$, appartenant respectivement à h classes quelconques mais différentes $F_{i_1}, F_{i_2}, \dots, F_{i_h}$, le nombre d'éléments x de E tels que :

$$(x, y^1) \in R, (x, y^2) \in R, \dots, \text{ et } (x, y^h) \in R \text{ est égal à :}$$

$$- q^{k-2} \text{ ou } q^{k-3}, \dots, \text{ ou } q^{k-h}, \text{ ou } 0, \text{ si } k \geq h$$

$$- q^{k-2} \text{ ou } q^{k-3}, \dots, \text{ ou } 1, \text{ ou } 0, \text{ si } k < h.$$

$$d) \forall h, 2 < h \leq k, \exists (i_1, i_2, \dots, i_h) \in [1, N]^h, i_1 \neq i_2 \neq \dots \neq i_h$$

$$\forall (y^1, y^2, \dots, y^h) \in F_{i_1} \times F_{i_2} \times \dots \times F_{i_h} :$$

$$\text{Card} [x : x \in E, (x, y^1) \in R, (x, y^2) \in R, \dots, (x, y^h) \in R] = q^{k-h}$$

c'est-à-dire

Pour tout entier h tel que $2 < h \leq k$, il existe h classes différentes $F_{i_1}, F_{i_2}, \dots, F_{i_h}$ telles que pour tout ensemble de h éléments de F , $y^1, y^2, \dots, y^h$, appartenant chacun à chacune de ces classes, le nombre d'éléments x de E tels que :

$$(x, y^1) \in R, (x, y^2) \in R, \dots, \text{ et } (x, y^h) \in R$$

soit égal à q^{k-h} .

2) Définition géométrique des réseaux (R).

a) Définissons l'application f de F dans $P(E)$, ensemble des parties de E par :

$$y \longrightarrow f(y) = \{ x : x \in E, (x, y) \in R \}.$$

On fait ainsi correspondre à chaque élément y de F un sous-ensemble d'éléments x de E tels que $(x, y) \in R$. Il est facile de vérifier que l'application ainsi définie est injective en se référant aux propriétés de définition a) et b) des réseaux (R).

Effectivement, supposons par l'absurde que $f(y_1) = f(y_2)$ pour $y_1 \neq y_2$.

y_1 et y_2 ne peuvent appartenir à la même classe F_i sinon la propriété a) de définition serait contredite (il y aurait des éléments x de E tels que $(x, y_1) \in R$ et $(x, y_2) \in R$ pour y_1 et y_2 appartenant à une même classe F_i , ce qui est impossible).

Supposons alors que $y_1 \in F_i$ et que $y_2 \in F_j$, $i \neq j$. Par application de la propriété de définition b) on a dans ce cas :

$$\text{Card} [x : x \in E, (x, y_1) \in R, (x, y_2) \in R] = q^{k-2}.$$

Si par l'absurde $f(y_1) = f(y_2)$ c'est que :

$$\text{Card} [x : x \in E, (x, y_1) \in R] =$$

$$\text{Card} [x : x \in E, (x, y_2) \in R] =$$

$$\text{Card} [x : x \in E, (x, y_1) \in R, (x, y_2) \in R] = q^{k-2}.$$

Soit alors un autre élément y'_2 de F_j .

On doit avoir également :

$$\text{Card} [x : x \in E, (x, y_1) \in R, (x, y'_2) \in R] = q^{k-2}.$$

Dans ces conditions, il existerait des éléments

x de E tels que : $(x, y_2) \in R$ et $(x, y'_2) \in R$ pour des éléments y_2 et y'_2 de F différents mais appartenant à une même classe F_j , ce qui est impossible (propriété a) de définition). Finalement donc : $y_1 \neq y_2 \implies f(y_1) \neq f(y_2)$ et l'application f est bien injective.

Il nous est alors possible d'identifier un élément y de F à son image $f(y)$.

F est alors identifié à une famille de parties de E et l'on peut définir une relation d'appartenance $\in$ des éléments de E aux éléments de F ainsi identifiés (à $f(F)$) par : $x \in y \iff (x, y) \in R$ (vue la définition de R , $(x, y) \in R$ implique nécessairement que $x \in E$ et $y \in F$).

b) Si nous désignons par

- points, les éléments de E
- plans, les éléments de F

$F_1, F_2, \dots, F_N$ étant N classes de plans, 2)a) nous permet d'employer un langage géométrique pour définir les réseaux (R) . Ce sera le suivant :

Soit E un ensemble fini d'éléments désignés par des points.

Soit F un sous-ensemble d'éléments de $P(E)$ désignés par des plans.

Soit $F_i, i \in [1, N]$, une partition de F en N classes F_i , ($\text{Card } [F_i] \geq 2$)

Soient q et k , 2 nombres entiers positifs ($2 < k < N$).

Le système $(E, F, F_i, i \in [1, N], R, k, q)$ constitue un réseau (R) de dimension k si les propriétés suivantes sont vérifiées :

(1) - Tout point x de E appartient à un plan y et un seul de chaque classe F_i .

(2) - Le nombre de points x de E appartenant à deux plans quelconques de deux classes différentes est égal à q^{k-2} .

(3) - Le nombre de points x de E appartenant à h plans quelconques de h classes différentes est égal :

- soit à q^{k-2} , soit à q^{k-3} , ... , soit à q^{k-h} , soit à 0,
si $2 < h \leq k$.

- soit à q^{k-2} , soit à q^{k-3} , ... , soit à 1 , soit à 0,
si $h > k$.

(4) - Pour tout entier h ($2 < h \leq k$), il existe h classes de plans différents telles que le nombre de points x de E appartenant à h plans quelconques de chacune de ces h classes soit égal à q^{k-h} .

Remarques.

a) Par la suite, quand on emploiera le langage géométrique, on dira de façon indifférente qu'un point x appartient à un plan y ou qu'un plan y passe par un point x .

b) De même, si un point x appartient à plusieurs plans $y_1, y_2, \dots, y_h$, on dira que x appartient à l'intersection des plans $y_1, y_2, \dots, y_h$ notée $y_1 \cap y_2 \cap \dots \cap y_h$ ou que $y_1 \cap y_2 \cap \dots \cap y_h$ passe par x .

(Ce qui n'est possible que parce que chaque plan a été identifié, rappelons-le, à un élément de $q(E)$; le signe $\cap$ est donc entendu dans sa signification usuelle).

c) On dira que h plans $y_1, y_2, \dots, y_h$ se coupent suivant $y_1 \cap y_2 \cap \dots \cap y_h$ entendant par là :

$\{x : x \in E, x \in y_1, x \in y_2, \dots, x \in y_h\}$ ou ce qui revient au même :

$\{x : x \in E, (x, y_1) \in R, \dots, (x, y_h) \in R\}$ selon la première terminologie.

d) $\text{Card } [y_1 \cap y_2 \cap \dots \cap y_h]$ désignera le nombre de points de l'intersection des plans $y_1, y_2, \dots, y_h$ (que l'on avait tout d'abord désigné par :

$\text{Card } [x : x \in E, (x, y_1) \in R, \dots, (x, y_h) \in R]$).

e) On dira que deux plans y_1 et y_2 sans points communs sont parallèles. L'application des propriétés de définition des réseaux a) et b) montre que deux plans de deux classes différentes ne sont pas parallèles (puisque se coupant toujours en q^{k-2} points), mais que deux plans quelconques d'une même classe le sont toujours (sinon par un point x de E pourraient passer deux plans d'une même classe).

En résumé, les plans d'une même classe, n'ayant pas de point commun, sont nécessairement parallèles.

La relation de parallélisme $\parallel : y_1 \parallel y_2 \iff \text{Card}[y_1 \cap y_2] = 0 \text{ ou } y_1 = y_2$ est évidemment une relation d'équivalence, puisqu'étant symétrique, réflexive et transitive ($y_1 \parallel y_2, y_2 \parallel y_3 \implies y_1 \parallel y_3$, ce qui est vérifié puisque nécessairement y_1, y_2 et y_3 appartiennent à une même classe).

On peut remarquer dès maintenant que les classes d'équivalence de cette relation de parallélisme ne sont autres que les classes F_i et que les plans d'une même classe constituent une partition de E , ceci en vertu de la propriété a) de définition des réseaux. (Effectivement, soit un plan y_1 de la classe F_i . Soit alors x_2 un point de E n'appartenant pas à y_1 ; il existe un plan de F_i , y_2 et un seul passant par x_2 . Soit ensuite x_3 un point de E , n'appartenant ni à y_1 ni à y_2 ; il existe un plan de F_i , y_3 et un seul passant par x_3 ; etc... Finalement :

$$E = \bigcup_{\forall y_j \in F_i} y_j, \quad \forall i \in [1, N])$$

3) Propriétés des Réseaux (R).

1° Propriété - Chaque classe F_i contient le même nombre n de plans ($\forall i \in [1, N]$).

Démonstration.

Soit un plan y_i d'une classe F_i et soient deux autres classes de plans F_j et F_1 .

$$\forall y_j \in F_j, \text{ on a } \text{Card} [y_i \cap y_j] = q^{k-2}$$

$$\forall y_1 \in F_1, \text{ on a } \text{Card} [y_i \cap y_1] = q^{k-2}$$

(de par la propriété b) de définition).

Désignons par n_j et n_1 les nombres respectifs de plans des classes F_j et F_1 . On a, en appliquant la propriété a) de définition :

$$y_i = \bigcup_{\forall y_j \in F_j} y_i \cap y_j \quad \text{et} \quad y_i = \bigcup_{\forall y_1 \in F_1} y_i \cap y_1$$

c'est-à-dire :

$$\text{Card} [y_i] = \sum_{\forall y_j \in F_j} \text{Card} [y_i \cap y_j] = n_j \cdot q^{k-2}$$

$$\text{Card} [y_i] = \sum_{\forall y_1 \in F_1} \text{Card} [y_i \cap y_1] = n_1 \cdot q^{k-2}$$

Soit : $n_j = n_1 = n$.

c. q. f. d.

2° Propriété. - Chaque classe F_i contient q plans ($\forall i \in [1, N]$).

Démonstration.

Vue la première propriété, il suffit de démontrer qu'une classe particulière de plans contient q plans.

Appliquons alors la propriété d) de définition : il est possible de trouver trois classes de plans F_i, F_j, F_1 telles que : $\forall y_i \in F_i, \forall y_j \in F_j, \forall y_1 \in F_1,$

$$\text{Card} [y_i \cap y_j \cap y_1] = q^{k-3}.$$

D'autre part, $\text{Card} [y_i \cap y_j] = q^{k-2}$ (propriété b) de définition) et l'on a :

$$y_i \cap y_j = \bigcup_{\forall y_1 \in F_1} y_i \cap y_j \cap y_1 \quad (\text{propriétés a) et d) de définition}).$$

Donc : $q^{k-2} = n q^{k-3}$ d'où $n = q$.

Le nombre de plans de la classe F_1 est finalement égal à q et le résultat annoncé suit en appliquant la première propriété c. q. f. d.

3° Propriété - Chaque plan d'un réseau contient q^{k-1} points.

Démonstration.

Soit y un plan quelconque du réseau et F_i une classe de plans à laquelle y n'appartient pas.

$$\text{On a : } y = \bigcup_{\forall y_i \in F_i} y \cap y_i$$

$$\text{D'où : } \text{Card } [y] = q \times q^{k-2} = q^{k-1}$$

4° Propriété - $\text{Card } [E] = q^k$

Démonstration.

On a vu que les plans de chaque classe constituaient une partition de E , c'est-à-dire :

$$E = \bigcup_{\forall y_i \in F_i} y_i$$

$$\text{Donc : } \text{Card } [E] = q \times q^{k-1} = q^k$$

5° Propriété -

Soient $y_1, y_2, \dots, y_h$, h plans d'un réseau (R) tels que :

$$\text{Card } [y_1 \cap y_2 \cap \dots \cap y_h] = q^{k-i} \quad (i \leq h).$$

Il est alors possible d'extraire i plans $y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_i}$ des h plans précédents, tels que :

$$y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_i} = y_1 \cap y_2 \cap \dots \cap y_h.$$

Démonstration.

Remarquons que la propriété est vérifiée pour $i = 2$.

Faisons alors un raisonnement par récurrence supposant la propriété exacte jusqu'au rang $i-1$. Soient alors h plans $y_1, y_2, \dots, y_h$ tels que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = q^{k-i} \quad (i \leq h).$$

- Supposons tout d'abord que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = q^{k-i+j} \quad \text{avec } j > 1.$$

On peut, en vertu de l'hypothèse de récurrence, extraire $i-j$ plans $y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{i-j}}$ des plans $y_1, y_2, \dots, y_{h-1}$, tels que :

$$\text{Card} [y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-j}}] = q^{k-i+j}$$

et plus précisément que :

$$y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-j}} = y_1 \cap y_2 \cap \dots \cap y_{h-1}.$$

Mais alors, la propriété de définition des réseaux c) est mise en défaut, si $j > 1$, puisque : $\text{Card} [y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-j}} \cap y_h]$ doit être égal à q^{k-i} (et qu'il ne peut ici être égal qu'à q^{k-i+j} ou $q^{k-i+j-1}$).

La seule possibilité est donc que j soit égal à 1, c'est-à-dire que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = q^{k-i+1}.$$

$y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{i-j}}$ et y_h constituent alors la famille de plans cherchée, c'est-à-dire telle que :

$$y_1 \cap y_2 \cap \dots \cap y_h = y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-1}} \cap y_h$$

- Si l'on suppose maintenant que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = q^{k-i},$$

on peut alors éliminer le plan y_h et recommencer le même raisonnement pour les plans $y_1, y_2, \dots, y_{h-1}$ restants. D'où la propriété énoncée. c. q. f. d.

6° Propriété - De tout réseau (R) on peut extraire k classes de plans :

$Fi_1, Fi_2, \dots, Fi_k$ telles que :
 $\forall y^{(1)} \in Fi_1, \forall y^{(2)} \in Fi_2, \dots, \forall y^{(k)} \in Fi_k$ et pour
 toute permutation $\alpha(1) \alpha(2) \dots \alpha(k)$ de $(1, 2, \dots, k)$,
 l'on ait :

$$\begin{aligned} \text{Card } [y^{\alpha(1)} \cap y^{\alpha(2)} \cap y^{\alpha(3)}] &= q^{k-3} \\ \vdots \\ \text{Card } [y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(h)}] &= q^{k-h} \\ \vdots \\ \text{Card } [y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(k)}] &= 1. \end{aligned}$$

Démonstration.

En vertu de la propriété d) de définition, on peut extraire du réseau k classes de plans $Fi_1, Fi_2, \dots, Fi_k$ telles que :

$$\begin{aligned} \forall y^{(1)} \in Fi_1, \forall y^{(2)} \in Fi_2, \dots, \forall y^{(k)} \in Fi_k, \text{ l'on ait :} \\ \text{Card } [y^{(1)} \cap y^{(2)} \cap \dots \cap y^{(k)}] &= 1. \end{aligned}$$

Soit $\alpha(1) \alpha(2) \dots \alpha(k)$ une permutation de $(1, 2, \dots, k)$
 On a de la même façon

$$(1) \text{ Card } [y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(k)}] = 1$$

Supposons alors par l'absurde que :

$$\text{Card } [y^{\alpha(1)} \cap \dots \cap y^{\alpha(k-1)}] = q^\beta \text{ avec } \beta > 1.$$

Dans ces conditions, en appliquant la 5° Propriété, on sait que l'on peut extraire $k-\beta$ plans $y^{\alpha(i_1)}, y^{\alpha(i_2)}, \dots, y^{\alpha(i_{k-\beta})}$ des plans précédents tels que :

$$\begin{aligned} \text{Card } [y^{\alpha(i_1)} \cap y^{\alpha(i_2)} \cap \dots \cap y^{\alpha(i_{k-\beta})}] &= q^\beta \text{ et que :} \\ y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(k-1)} &= y^{\alpha(i_1)} \cap y^{\alpha(i_2)} \cap \dots \cap y^{\alpha(i_{k-\beta})} \end{aligned}$$

En ajoutant le plan $y^{\alpha(k)}$, on ne pourra donc obtenir la relation (1) (en vertu de la propriété c) de définition).

On aboutit donc à une contradiction.

Finalement on doit avoir :

$$\text{Card} [y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(k-1)}] = q.$$

Le même raisonnement peut alors être répété, d'où la propriété énoncée. c. q. f. d.

7° Propriété - Soient dans un réseau (R) k classes de plans $Fi_1, Fi_2, \dots, Fi_k$ telles que :

$$\forall y^{(1)} \in Fi_1, \forall y^{(2)} \in Fi_2, \dots, \forall y^{(k)} \in Fi_k, \text{ l'on ait : } \\ \text{Card} [y^{(1)} \cap y^{(2)} \cap \dots \cap y^{(k)}] = 1$$

Alors :

$$\text{Card} [y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(h)}] = q^{k-h} \\ \forall h \in [2, k], \forall \alpha(1), \alpha(2), \dots, \alpha(h) \in [1, k] \\ \alpha(1) \neq \alpha(2) \neq \dots \neq \alpha(k).$$

La démonstration de cette propriété est incluse dans la démonstration de la propriété précédente.

Remarques.

=====

α) En résumé, un réseau (R) sera nécessairement constitué par un ensemble E de q^k points et un ensemble F de N classes de q plans parallèles, chaque plan contenant q^{k-1} points (cela n'est bien sûr pas suffisant).

β) Nous nous sommes placés dans l'énoncé de toutes les propriétés précédentes dans le cas de la définition qui était celui d'un réseau (R) à k dimensions.

4) Définition des réseaux $(R)_{k-1}$.

Un réseau $(R)_{k-1}$ est un réseau (R) à k dimensions, possédant la propriété supplémentaire suivante :

$$\forall (x_1, x_2) \in E^2, x_1 \neq x_2 : \text{Card} [y : y \in F, (x_1, y) \in R, (x_2, y) \in R] \leq k-1$$

Cette propriété peut s'énoncer ainsi géométriquement.
Par tout couple de points, il ne passe pas plus de $k-1$ plans. On a alors le résultat suivant :

Théorème.

$$\begin{aligned} & \forall h > 2, \forall (i_1, i_2, \dots, i_h) \in [1, N]^h, i_1 \neq i_2 \neq \dots \neq i_h \\ & \forall (y^1, y^2, \dots, y^h) \in Fi_1 \times Fi_2 \times \dots \times Fi_h \\ & \text{Card} [x : x \in E, (x, y^1) \in R, (x, y^2) \in R, \dots, (x, y^h) \in R] = \\ & - q^{k-h} \quad \text{si } k \geq h \\ & - \text{soit } 1, \text{ soit } 0 \quad \text{si } h > k. \end{aligned}$$

Autrement dit : h plans quelconques de h classes différentes se coupent en q^{k-h} points si $h \leq k$ ou alors, soit en un point, soit en zéro point si $h > k$.

Démonstration.

Remarquons en premier lieu que si $h \geq k$, il n'y a rien à démontrer vue la définition des réseaux $(R)_{k-1}$.
Plaçons-nous en conséquence dans le cas où $h < k$.
Soient donc h plans $y_1, y_2, \dots, y_h$ avec $h < k$.

$$\begin{aligned} & \alpha) \text{ Supposons tout d'abord par l'absurde que :} \\ & \text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] > q^{k-h}, \text{ soit par exemple :} \\ & \text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = q^{k-h+j} \text{ avec } j > 0. \end{aligned}$$

Par application de la 5° propriété, on sait que l'on peut extraire des h plans précédents $h-j$ plans $y_{\alpha(1)} \dots y_{\alpha(h-j)}$ tels que :

$$\text{Card} [y_{\alpha(1)} \cap y_{\alpha(2)} \cap \dots \cap y_{\alpha(h-j)}] = q^{k-h+j}$$

Soit alors un autre plan du réseau, z_1 , coupant $y_1 \cap y_2 \cap \dots \cap y_h$ (z_1 existe en vertu de la propriété de définition a) et puisque $N > k$).

On a :

$$\begin{aligned} \text{Card} [y_{\alpha(1)} \cap \dots \cap y_{\alpha(h-j)} \cap z_1] &= \text{Card} [y_1 \cap y_2 \cap \dots \cap y_h \cap z_1] \\ &\geq q^{k-h+j-1} \end{aligned}$$

c'est-à-dire :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h \cap z_1] > q^{k-h-1}$$

En répétant ce procédé $k-h$ fois, ce qui est possible puisque $N > k$, on peut exhiber $k-h$ plans du réseau, $z_1, z_2, \dots, z_{k-h}$ tels que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h \cap z_1 \cap z_2 \cap \dots \cap z_{k-h}] > 1$$

Dans ces conditions, il passerait k plans par certains couples de points du réseau, ce qui contredit la définition des réseaux $(R)_{k-1}$.

La seule possibilité si $y_1 \cap y_2 \cap \dots \cap y_h \neq \emptyset$ est donc que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = q^{k-h}$$

(β) Supposons maintenant par l'absurde que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = 0 \quad (\text{toujours dans le cas } h < k).$$

On peut toujours se ramener au cas :

$$y_1 \cap y_2 \cap \dots \cap y_h = \emptyset \quad \text{avec} \quad y_1 \cap y_2 \cap \dots \cap y_{h-1} \neq \emptyset.$$

Si $y_1 \cap y_2 \cap \dots \cap y_{h-1} \neq \emptyset$, d'après ce qui précède, on a :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = q^{k-h+1}$$

Soit $x \in y_1 \cap y_2 \cap \dots \cap y_{h-1}$ et soit y_h^1 un plan parallèle à y_h passant par x . Puisque $\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h^1] \neq 0$, on a :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h^1] = q^{k-h}$$

Or $y_1 \cap y_2 \cap \dots \cap y_{h-1}$ est réunion des ensembles : $y_1 \cap \dots \cap y_{h-1} \cap z$ où z parcourt les plans parallèles à y_h . Par suite

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = \sum_{\forall z \parallel y_h} \text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1} \cap z]$$

D'après ce qui précède, cette égalité s'écrit :

$$q^{k-h+1} = m q^{k-h} \quad \text{si } m \text{ plans parallèles à } y_h$$

coupent $y_1 \cap y_2 \cap \dots \cap y_{h-1}$ ($m \leq q-1$).

Il y a donc contradiction puisque l'égalité précédente implique $m = q$.

Finalement si $h < k$, il est impossible que l'ensemble $y_1 \cap y_2 \cap \dots \cap y_h$ soit vide, donc :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = q^{k-h} \quad \text{c.q.f.d.}$$

On a en particulier pour les réseaux $(R)_{k-1}$ de dimension k la propriété remarquable que k plans de k classes différentes définissent un point. Ces réseaux, en résumé, sont caractérisés par les propriétés a) et b) de définition et par le théorème précédent.

5) Définitions des réseaux $(R)_t$.

Un réseau $(R)_t$ de dimension k sera un réseau (R) de dimension k possédant la propriété supplémentaire suivante :

$$\forall (x_1, x_2) \in E^2, x_1 \neq x_2, \text{Card} [y : y \in F, (x_1, y) \in R, (x_2, y) \in R] \leq t$$

$$(t > k-1),$$

propriété pouvant s'énoncer géométriquement ainsi :

Par tout couple de points d'un réseau $(R)_t$, il ne passe pas plus de t plans. Il n'y a pas de résultat particulier à dégager dans ce cas sinon que $t+1$ plans définiront au plus un point.

6) Définition des réseaux $(\hat{R})$.

Un réseau $(\hat{R})$ est un réseau (R) vérifiant la propriété suivante :

$$\exists F_{i_1}, F_{i_2}, \dots, F_{i_k} \quad i_1 \neq i_2 \neq \dots \neq i_k$$

$$\forall (j_1, j_2, \dots, j_{k-1}) \subset \{i_1, i_2, \dots, i_k\}, j_1 \neq j_2 \neq \dots \neq j_{k-1}$$

$$\forall (y_1, y_2, \dots, y_{k-1}) \in F_{j_1} F_{j_2} \dots F_{j_{k-1}}$$

$$\forall y \notin F_{j_1} F_{j_2} \dots F_{j_{k-1}}$$

$$\implies \text{Card} [y_1 \cap y_2 \cap \dots \cap y_{k-1} \cap y] = 1$$

Autrement dit, de tout réseau $(\hat{R})$, on peut extraire k classes de plans telles que pour tout ensemble de $k-1$ plans $y_1, y_2, \dots, y_{k-1}$ pris dans $k-1$ de ces classes et pour tout plan y pris dans l'une quelconque des $N-k+1$ classes restantes, l'on ait :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{k-1} \cap y] = 1.$$

Remarques.

- a) Cette définition suppose le réseau (R) de dimension k , ce qui était supposé dans la définition des réseaux (R) .
- b) Il est facile de montrer en utilisant les propriétés 5, 6 et 7 que cette propriété des réseaux $(\hat{R})$ entraîne la propriété d) de définition des réseaux (R) .

Un réseau $(\hat{R})$ peut donc être défini par la propriété précédente jointe aux trois premières propriétés de définition des réseaux (R) .

- c) Un réseau $(\hat{R})_t$ est évidemment un réseau $(\hat{R})$ possédant la propriété précédente de définition des réseaux $(R)_t$.

II. Définition des arrangements (T_k) et application aux réseaux (R) .

On va étudier une représentation analytique des réseaux (R) , c'est-à-dire, chercher à associer une équation à chaque plan et des coordonnées à chaque point.

1) - Définition des arrangements (T_k) .

Soit X un ensemble de q éléments. Soit k un entier supérieur ou égal à deux. Soit f une application de X^k dans X :

$$(x_1, x_2, \dots, x_k) \in X^k \xrightarrow{f} y = f(x_1, x_2, \dots, x_k) \in X$$

possédant la propriété suivante :

$$\forall (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_k) \in X^{k-1}, \forall i \in [1, k],$$

l'application : $g(x) = f(a_1, a_2, \dots, a_{i-1}, x, a_{i+1}, \dots, a_k)$ de X dans X est une bijection de X sur X .

Autrement dit, l'application $y = f(x_1, x_2, \dots, x_k)$ de X^k dans X est une bijection de X sur X quand $k-1$ variables x_i quelconques sont déjà fixées et que la variable x_i restante seule varie dans X .

On définit ainsi un arrangement (T_k) noté :

$$[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)] \quad , \quad x_i \in X, \forall i \in [1, k]$$

2) - Propriétés des arrangements (T_k) .

Il est immédiat de constater les propriétés suivantes :

a) L'équation suivante, où x est seule variable :

$$f(a_1, a_2, \dots, a_{i-1}, x, a_{i+1}, \dots, a_k) = b$$

a une solution et une seule, $\forall (a_1, a_2, \dots, a_k, b) \in X^k, \forall i \in [1, k]$

b) L'équation : $f(x_1, x_2, \dots, x_k) = b$, où $x_1, x_2, \dots, x_k$ sont tous variables admet q^{k-1} solutions, $\forall b \in X$.

De façon générale, l'équation : $f(x_1, x_2, \dots, x_k) = b$, où $x_{i_1}, x_{i_2}, \dots, x_{i_h}$ sont seules variables, les autres x_j et b ayant leurs valeurs fixées dans X admet q^{h-1} solutions, ($\forall h \in [1, k]$).

Effectivement, la propriété a) est équivalente au fait que $g(x) = f(a_1, a_2, \dots, a_{i-1}, x, a_{i+1}, \dots, a_k)$ est une bijection de X sur X , $\forall (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_k) \in X^{k-1}$ et la propriété b) est une conséquence de a) : en effet, supposons $x_{i_1}, x_{i_2}, \dots, x_{i_{h-1}}$ fixées, x_{i_h} étant seule variable.

Par application de a), $f(x_1, x_2, \dots, x_k) = b$ a une solution et une seule et ceci quelles que soient les valeurs fixées de $x_{i_1}, x_{i_2}, \dots, x_{i_{h-1}}$; d'où les q^{h-1} solutions annoncées.

3) - Définition des arrangements (T_k) orthogonaux.

Soit une famille de h arrangements (T_k) sur un

ensemble X de k éléments :

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)] , x_j \in X \quad \forall j \in [1, k] \quad i \in [1, h]$$

On dira que ces h arrangements (T_k) forment une famille d'arrangements orthogonaux si et seulement si la propriété suivante est satisfaite :

$$I \begin{cases} f_1(x_1, x_2, \dots, x_k) = a^1 \\ f_2(x_1, x_2, \dots, x_k) = a^2 \\ \dots \\ f_h(x_1, x_2, \dots, x_k) = a^h \end{cases}$$

Tous les systèmes extraits de I , à i équations et à i inconnues : $(x_{t_1}, x_{t_2}, \dots, x_{t_i}) \in X^i$ ont une solution et une seule et ceci pour tout i

$(i = 1, 2, \dots, \min [h, k])$, pour tout $a^j \in X$,

$(j = 1, 2, \dots, \min [h, k])$, les autres x_i ayant des valeurs fixées quelconques dans X .

4 - Equivalence entre arrangements (T_k) orthogonaux et réseaux $(R)_{k-1}$.

Théorème 1.

L'existence de h arrangements (T_k) orthogonaux, construits sur un ensemble X de q éléments entraîne l'existence d'un réseau $(R)_{k-1}$ de q^k points et de $N = k+h$ classes de q plans parallèles.

Démonstration.

Désignons les q éléments de X par $a_1, a_2, \dots, a_q$. les k -tuples $(x_1, x_2, \dots, x_k)$, $x_i \in X$, $i \in [1, k]$, constituent les q^k points du réseau $(R)_{k-1}$.

D'autre part, le nombre de solutions de l'équation : $x_i = a_i$ (a_i fixé dans X) est égal à q^{k-1} (nombre de k -tuples $(x_1, x_2, \dots, x_k)$ vérifiant $x_i = a_i$).

Dans ces conditions $x_i = a_i$ sera prise comme l'équation d'un certain plan.

D'où, tout d'abord, k classes de q plans :

$$\text{la } \underline{1}^{\text{ère}} \text{ classe} \left\{ \begin{array}{ll} x_1 = a_1 & (1^{\circ} \text{ plan}) \\ x_1 = a_2 & (2^{\circ} \text{ plan}) \\ \vdots & \\ x_1 = a_q & (q^{\circ} \text{ plan}) \end{array} \right.$$

. . .

$$\text{la } \underline{i}^{\text{ème}} \text{ classe} \left\{ \begin{array}{ll} x_i = a_1 & (1^{\circ} \text{ plan}) \\ x_i = a_2 & (2^{\circ} \text{ plan}) \\ \vdots & \\ x_i = a_q & (q^{\circ} \text{ plan}) \end{array} \right.$$

. . .

$$\text{la } \underline{k}^{\text{ème}} \text{ classe} \left\{ \begin{array}{ll} x_k = a_1 & (1^{\circ} \text{ plan}) \\ x_k = a_2 & (2^{\circ} \text{ plan}) \\ \vdots & \\ x_k = a_q & (q^{\circ} \text{ plan}) \end{array} \right.$$

On a vu également que le nombre de solutions de l'équation : $f_i(x_1, x_2, \dots, x_k) = a$, $\forall i \in [1, h]$, $\forall a \in X$ quand $x_1, x_2, \dots, x_k$ sont tous variables est égal à q^{k-1} . Dans ces conditions : $f_i(x_1, x_2, \dots, x_k) = a$, a fixé, sera prise comme l'équation d'un certain plan.

D'où h classes de q plans s'ajoutant aux k classes précédentes.

$$\text{la } 1^{\text{ère}} \text{ classe} \left\{ \begin{array}{ll} f_1(x_1, x_2, \dots, x_k) = a_1 & (1^{\circ} \text{ plan}) \\ \vdots & \\ f_1(x_1, x_2, \dots, x_k) = a_q & (q^{\circ} \text{ plan}) \end{array} \right.$$

. . .

$$\text{la } i^{\text{ème}} \text{ classe} \begin{cases} f_i(x_1, x_2, \dots, x_k) = a_1 & (1^{\circ} \text{ plan}) \\ \vdots \\ f_i(x_1, x_2, \dots, x_k) = a_q & (q^{\circ} \text{ plan}) \end{cases}$$

...

$$\text{la } h^{\text{ème}} \text{ classe} \begin{cases} f_h(x_1, x_2, \dots, x_k) = a_1 & (1^{\circ} \text{ plan}) \\ \dots \\ f_h(x_1, x_2, \dots, x_k) = a_q & (q^{\circ} \text{ plan}) \end{cases}$$

En résumé, on a donc construit un ensemble E de q^k points et un ensemble F de parties de E, soit $h+k$ classes de q plans contenant chacun q^{k-1} points.

On doit maintenant vérifier les propriétés de définition des réseaux $(R)_{k-1}$ sur ces données.

α) Par tout point, il passe un plan et un seul de chaque classe.

Soit $(x_1, x_2, \dots, x_k)$ un point quelconque. Soit la classe de plans $x_i = a$: il n'y a bien évidemment qu'une seule possibilité.

Soit la classe de plans $f_i(x_1, x_2, \dots, x_k) = a$: il n'y a encore une fois qu'une seule possibilité, sinon $f_i(x_1, x_2, \dots, x_k)$ serait égal à a_i ou a_j ($a_i \neq a_j$), ce qui contredit la définition de $f_i(x_1, x_2, \dots, x_k)$

(qui est en particulier une application).

β) Deux plans de deux classes différentes se coupent en q^{k-2} points.

Cela est évident pour des plans $x_i = a$ et $x_j = b$ ($\forall (a, b) \in X^2$).

- Soient deux plans $x_i = a$ et $f_j(x_1, x_2, \dots, x_k) = b$
 x_i est fixé à a , d'où q^{k-2} solutions pour l'équation
 $f_j(x_1, x_2, \dots, a, \dots, x_k) = b$.

- Soient deux plans $f_i(x_1, x_2, \dots, x_k) = a$
 et $f_j(x_1, x_2, \dots, x_k) = b$

Fixons par exemple $x_3, x_4, \dots, x_k$. En utilisant la propriété des arrangements (T_k) d'être orthogonaux, le système

$$\begin{cases} f_i(x_1, x_2, \dots, x_k) = a \\ f_j(x_1, x_2, \dots, x_k) = b \end{cases}$$

a une solution et une seule en (x_1, x_2) . Ceci étant valable quelle que soit la fixation de $(x_3 \dots x_k)$, il y a donc q^{k-2} solutions.

7) Soient maintenant h_1 plans.

- i plans du type $x_j = \alpha_j \quad (\alpha_j \in X)$
 - $h_1 - i$ plans du type $f_i(x_1, x_2, \dots, x_k) = \alpha_i \quad (\alpha_i \in X)$

Supposons $h_1 \leq k$. Ces h_1 plans conduisent à l'étude d'un système de $h_1 - i$ équations à $k - i$ inconnues :

$$\begin{cases} f_{i_1}(x_1, x_2, \dots, x_k) = \alpha_{i_1} \\ \dots \\ f_{i_{h_1-i}}(x_1, x_2, \dots, x_k) = \alpha_{i_{h_1-i}} \end{cases}$$

Fixons dans ce système $k - h_1$ inconnues parmi les $k - i$ inconnus. Il reste donc un système de $h_1 - i$ équations à $h_1 - i$ inconnues qui a une solution et une seule. D'où q^{k-h_1} solutions pour le système proposé et le fait que h_1 plans de h_1 classes différentes se coupent en q^{k-h_1} points quand $h_1 \leq k$ en découle immédiatement.

La vérification du cas où $h_1 > k$ est aussi simple. On a donc bien construit le réseau $(R)_{k-1}$ annoncé. c.q.f.d.

Théorème 2.

L'existence d'un réseau $(R)_{k-1}$ de q^k points et de

$N = h+k$ classes de q plans parallèles entraîne l'existence de h arrangements (T_k) orthogonaux, construits sur un ensemble X de q éléments.

Démonstration.

α) Choisissons k classes de plans arbitraires du réseau $(R)_{k-1}$, soient : Fi_1 , Fi_2 , ... , Fi_k .

On a vu que k plans, pris dans chacune de ces k classes définissent un point x et un seul de E (réseau $(R)_{k-1}$ page 14). Soit d'autre part X , un ensemble de q éléments. Mettons en correspondance biunivoque avec X , les q plans de chacune des k classes précédentes. (Cela revient à une bijection près à numéroter les q plans de chacune des k classes précédentes de 1 à q).

Si le point x de E est l'intersection :

- du plan repéré par x_1 , dans la classe Fi_1
- du plan repéré par x_2 , dans la classe Fi_2
- ...
- du plan repéré par x_k , dans la classe Fi_k ,

on fera correspondre à x l'élément $(x_1, x_2, \dots, x_k)$ de X^k . Ainsi, en ayant utilisé k classes de plans, on a pu associer à tous les points du réseau $(R)_{k-1}$ des coordonnées ; ces coordonnées sont distinctes pour deux points différents puisque k plans définissent un point et un seul. En résumé, la correspondance établie entre E et X^k est une bijection de E sur X^k .

β) Il s'agit maintenant de vérifier tout d'abord que chacune des h classes restantes permet de définir un arrangement (T_k) : $(x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k))$
 $\forall i \in [1, h]$, $(x_1, x_2, \dots, x_k) \in X^k$.

Comme précédemment, mettons en correspondance biunivoque avec X , les q plans de chacune des h classes restantes. Considérons alors la $i^{\text{ème}}$ classe : ses q plans sont donc repérés par chacun des éléments de X .

En désignant les éléments de X par $a_1, a_2, \dots, a_q$, les q plans de la $i^{\text{ème}}$ classe sont donc repérés respectivement par $a_1, a_2, \dots$ et a_q , par exemple.

On sait d'autre part que chacun de ces q plans contient q^{k-1} points et que leur ensemble constitue une partition de E .

On peut donc en utilisant les plans de la $i^{\text{ème}}$ classe définir une application de X^k dans X qui fera correspondre au point de E coordonné par $(x_1, x_2, \dots, x_k)$, $f_i(x_1, x_2, \dots, x_k)$, $f_i(x_1, x_2, \dots, x_k)$ désignant l'élément de X repérant le plan de la classe i passant par $(x_1, x_2, \dots, x_k)$. Pour montrer que l'on a ainsi obtenu un arrangement (T_k) :

$(x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k))$,
il reste à vérifier que l'équation :

$$f_i(a_1, a_2, \dots, a_{j-1}, X, a_j, \dots, a_k) = a_\alpha$$

a une solution et une seule en X et ceci :

$$\forall a_\alpha \in X \quad , \quad \forall (a_1, a_2, \dots, a_{j-1}, a_{j+1}, \dots, a_k) \in X^{k-1}, \forall j \in [1, k]$$

Ceci est équivalent au fait que k plans définissent un point et un seul pourvu qu'ils soient k classes différentes.

(Effectivement, il s'agit ici de l'intersection des k plans suivants :

$$x_1 = a_1, x_2 = a_2, \dots, x_{j-1} = a_{j-1}, x_{j+1} = a_{j+1}, \dots, x_k = a_k$$

et $f_i(x_1, x_2, \dots, x_k) = a_\alpha$).

Ce travail, pouvant être effectué pour chacune des h classes de plans restantes, on a donc bien défini

h arrangements (T_k) :

$$(x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)) \quad \forall i \in [1, h]$$

Y) Il reste enfin à vérifier que les arrangements (T_k) construits sont orthogonaux.

Soit le système I suivant :

$$I \quad \begin{cases} f_1(x_1, x_2, \dots, x_k) = a_1 \\ f_2(x_1, x_2, \dots, x_k) = a_2 \\ \dots \\ f_h(x_1, x_2, \dots, x_k) = a_h \end{cases}$$

On a déjà remarqué que k plans de k classes différentes définissent un point et un seul : c'est cette propriété que nous allons utiliser encore une fois.

Soient k plans de k classes différentes, k-i étant du type :

$$\begin{cases} x_{i1} = a_{i1} \\ x_{i2} = a_{i2} \\ \dots \\ x_{i_{k-i}} = a_{i_{k-i}} \end{cases}$$

les i restants s'écrivant :

$$II \quad \begin{cases} f_{j1}(x_1, x_2, \dots, x_k) = a_{j1} \\ \dots \\ f_{ji}(x_1, x_2, \dots, x_k) = a_{ji} \end{cases}$$

Les deux faits : "les k plans précédents se coupent en un point et un seul" et "le système II de i équations à i inconnues x_j ($\forall j \neq i_1, i_2, \dots, i_{k-i}$) a une solution et une seule" sont équivalents.

Tout système de i équations à i inconnues extrait du système I a donc une solution et une seule et les arrangements (T_k) construits sont orthogonaux.

c. q. f. d.

5) - Généralisation : Equivalence entre réseaux $(\hat{R})_t$ et familles d'arrangements (T_k) .

Théorème 3.

Soit X un ensemble de q éléments. Soient $f_i(x_1, x_2, \dots, x_k)$, $i \in [1, h]$, h applications de X^k dans X , telles que l'on puisse construire h arrangements (T_k) sur X :

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)],$$

$$x_j \in X, \quad \forall j \in [1, k], \quad i \in [1, h]$$

Les propriétés suivantes sont équivalentes :

$$a) \quad \begin{cases} a^1 = f_1(x_1, x_2, \dots, x_k) \\ a^2 = f_2(x_1, x_2, \dots, x_k) \\ \dots \\ a^h = f_h(x_1, x_2, \dots, x_k) \end{cases} \quad I$$

- D'une façon générale, tout système de $h_1 - \alpha$ équations à $k - \alpha$ inconnues que l'on peut extraire du système I admet :

- si $h_1 \leq k$, $\alpha \leq h_1 - 3$, soit $q^{k - \alpha - 2}$, soit $q^{k - \alpha - 3}$, ... soit $q^{k - h_1}$, soit 0 solutions.

- si $h_1 > k$, $\alpha \leq k - 3$, soit $q^{k - \alpha - 2}$, soit $q^{k - \alpha - 3}$, ... soit 1, soit 0 solutions.

- D'une façon précise, tout système extrait de I , de $h + \alpha - t$ équations et de α inconnues a au plus une solution et une seule et ceci pour tout $\alpha = 2, 3, \dots, \min [t, k]$. En outre tout système de deux équations à k inconnues extrait du système I admet q^{k-2} solutions.

- On a $h > t$ et les résultats précédents sont vérifiés :

$$\forall (a^1, a^2, \dots, a^h) \in X^h.$$

b) Il existe un réseau $(\hat{R})_{h+k-t-1}$ de q^k points et de $h+k$ classes de q plans parallèles (Par tout couple de points, il ne passe pas plus de $h+k-t-1$ plans).

Démonstration.

On est forcé de poser $h > t$, puisque pour un réseau $(R)_t$ on avait l'inégalité $t > k-1$ qui s'écrit dans le cas présent : $h+k-t-1 > k-1$.

$$\alpha) \underline{a) \implies b)}.$$

La construction du réseau est analogue à celle effectuée dans la démonstration du théorème 1.

A chaque k -tuple $(x_1, x_2, \dots, x_k)$ de X^k , on associera un point du réseau. D'où q^k points.

Quant aux $h+k$ classes de plans, ce seront les suivantes :

$$\begin{array}{lcl}
 1^{\circ} \text{ classe} & \left\{ \begin{array}{l} x_1 = a_1 \quad (1^{\circ} \text{ plan}) \\ \dots \\ x_1 = a_q \quad (q^{\circ} \text{ plan}) \end{array} \right. \\
 \dots \\
 i^{\text{ème}} \text{ classe} & \left\{ \begin{array}{l} x_i = a_1 \quad (1^{\circ} \text{ plan}) \\ \dots \\ x_i = a_q \quad (q^{\circ} \text{ plan}) \end{array} \right. \\
 \dots \\
 k^{\text{ème}} \text{ classe} & \left\{ \begin{array}{l} x_k = a_1 \quad (1^{\circ} \text{ plan}) \\ \dots \\ x_k = a_q \quad (q^{\circ} \text{ plan}) \end{array} \right. \\
 \dots \\
 k+1^{\text{ème}} \text{ classe} & \left\{ \begin{array}{l} f_1(x_1, x_2, \dots, x_k) = a_1 \quad (1^{\circ} \text{ plan}) \\ \dots \\ f_1(x_1, x_2, \dots, x_k) = a_q \quad (q^{\circ} \text{ plan}) \end{array} \right. \\
 \dots \\
 k+h^{\text{ème}} \text{ classe} & \left\{ \begin{array}{l} f_h(x_1, x_2, \dots, x_k) = a_1 \quad (1^{\circ} \text{ plan}) \\ \dots \\ f_h(x_1, x_2, \dots, x_k) = a_q \quad (q^{\circ} \text{ plan}) \end{array} \right.
 \end{array}$$

(on a désigné les éléments de X par $a_1, a_2, \dots, a_q$).

Les propriétés a) et b) des définitions des réseaux (R) se démontrent de la même façon qu'elles ont été démontrées dans la démonstration du théorème 1, deux équations à k inconnues ayant q^{k-2} solutions, 2 plans de 2 classes différentes se couperont toujours en q^{k-2} points. Il reste à démontrer les propriétés c) et d), le fait que l'on a des réseaux $(\hat{R})$ et que ce sont des réseaux $(R)_{h+k-t-1}$

α) La propriété de définition d) est vérifiée en considérant les k premières classes de plans :

$$\left\{ \begin{array}{ll} x_1 = a & \forall a \in X \\ x_2 = a & \forall a \in X \\ \vdots & \\ x_k = a & \forall a \in X \end{array} \right.$$

Il est bien évident que h plans quelconques appartenant à h de ces k classes se coupent suivant q^{k-h} points, ceci étant valable pour $h = 2, 3, \dots, k$.

β) Le fait que l'on a des réseaux $(\hat{R})$ est également facile à établir en considérant toujours les k premières classes de plans précédentes. Dès lors, soit une autre classe de plans et un plan de cette classe :

$$f_i(x_1, x_2, \dots, x_k) = a_i.$$

Si l'on coupe ce plan avec par exemple : $x_1 = a_1, x_2 = a_2, \dots, x_{k-1} = a_{k-1}$, il est bien certain que l'on obtient un seul point comme intersection de ces k plans, ceci puisque $g(x) = f_i(a_1, a_2, \dots, a_{k-1}, x)$ est une bijection de X sur X .

γ) Démontrons maintenant la propriété c) de définition des réseaux. Soient h_1 plans de h_1 classes différentes. Supposons que α d'entre eux soient de la forme :

$$\begin{cases} x_{i1} = a_{i1} ; \\ x_{i2} = a_{i2} , \\ \dots \\ x_{i\alpha} = a_{i\alpha} , \end{cases}$$

les $h_1 - \alpha$ restants ayant pour équations :

$$\text{II} \quad \begin{cases} f_{j1}(x_1, x_2, \dots, x_k) = a_{j1} \\ f_{j2}(x_1, x_2, \dots, x_k) = a_{j2} \\ \dots \\ f_{jh_1-\alpha}(x_1, x_2, \dots, x_k) = a_{jh_1-\alpha} \end{cases}$$

Le système II est un système de $h_1 - \alpha$ équations extrait du système I et ayant $k - \alpha$ inconnues.

Par hypothèse, il peut admettre :

- soit $q^{k-\alpha-2}$, soit $q^{k-\alpha-3}$, ..., soit q^{k-h_1} , soit 0 solutions si $h_1 \leq k$,
- soit $q^{k-\alpha-2}$, soit $q^{k-\alpha-3}$, ..., soit 1, soit 0 solutions si $h_1 > k$.

Les h_1 plans des h_1 classes différentes, considérés peuvent donc se couper :

- soit en $q^{k-\alpha-2}$, soit en $q^{k-\alpha-3}$, ..., soit en q^{k-h_1} , soit en 0 points ; si $h_1 \leq k$
- soit en $q^{k-\alpha-2}$, soit en $q^{k-\alpha-3}$, ..., soit en 1, soit en 0 points, si $h_1 > k$.

La propriété c) de définition des réseaux (R) est donc établie. (Le cas particulier $\alpha = 0$ conduira au cas particulier de plans pouvant se couper en q^{k-2} points).

δ) Il n'y a plus à vérifier que l'on a des réseaux $(R)_{h+k-t-1}$. Ceci découle immédiatement du fait que tout système de $h+\alpha - t$ équations à α inconnues tiré du système I a au plus une solution, donc que tout système de $h+k-t$ plans définit au plus un point. En conséquence, par tout couple de

points, il ne passe pas plus de $h+k-t-1$ plans.

On a donc bien finalement un réseau $(\hat{R})_{h+k-t-1}$.

$\beta) \underline{b) \implies a)}$.

Il s'agit tout d'abord d'associer à chaque point des coordonnées, ce que l'on fera en utilisant les k classes de plans particulières que l'on sait exister dans un réseau $(\hat{R})$ (définition des réseaux $(\hat{R})$).

Le processus est identique à celui décrit dans la démonstration du théorème 2, et de façon absolument semblable, chacune des h classes de plans restantes permet de définir un arrangement (T_k) .

La propriété de définition des réseaux c) jointe au fait que les réseaux considérés sont par hypothèse des réseaux $(R)_{h+k-t-1}$ permet alors de déduire a) de b).

Ainsi par exemple, on sait que $h+k-t$ plans se coupent en au plus un point :

soient α de ces plans de la forme :

$$\begin{cases} x_{i1} = a_1 \\ x_{i2} = a_2 \\ \dots \\ x_{i\alpha} = a_{\alpha} \end{cases}$$

les $h+k-t-\alpha$ autres étant de la forme :

$$f_i(x_1, x_2, \dots, x_k) = a^i.$$

On est ramené à l'étude d'un système de $h+k-t-\alpha$ équations à $k-\alpha$ inconnues qui a au plus une solution.

De la même façon, en utilisant la propriété c) de définition, on montrerait que le nombre de solutions d'un système de $h_1-\alpha$ équations à $k-\alpha$ inconnues est égal aux nombres indiqués dans l'énoncé du théorème 3.

On a donc bien défini une famille de h arrangements (T_k) possédant les propriétés énoncées en a).

6) - Exemple d'arrangements (T_k) .

a) Définition d'une structure de quasi-groupe.

Soit X un ensemble de q éléments muni d'une loi de composition interne ϕ .

ϕ induit sur X une structure de quasi-groupe si les équations : $x\phi a = b$ ou $a\phi x = b$, ont une solution et une seule en x , quels que soient a et b .

b) Construction d'un arrangement (T_k) .

Soit donné un ensemble de q éléments : $X = \{a_1, a_2, \dots, a_q\}$
Soit ϕ_i , $i \in [1, k-1]$, une famille de $k-1$ opérations, induisant chacune sur X une structure de quasi-groupe. On considère alors l'application f de X^k sur X définie par :

$$(x_1, x_2, \dots, x_k) \in X^k \xrightarrow{f} [(x_1 \phi_1 x_2) \phi_2 x_3] \phi_3 \dots \phi_{k-1} x_k$$

On définit ainsi un arrangement (T_k) noté :

$$[x_1, x_2, \dots, x_k ; x_1 \phi_1 x_2 \phi_2 \dots \phi_{k-1} x_k]$$

$$x_i \in X, \forall i \in [1, k]$$

Justification.

- Remarquons tout d'abord que pour alléger l'écriture, on a écrit finalement : $x_1 \phi_1 x_2 \phi_2 \dots \phi_{k-1} x_k$ pour :

$$\{ [(x_1 \phi_1 x_2) \phi_2 x_3] \phi_3 \dots \} \phi_{k-1} x_k$$

Il est donc sous-entendu que l'on a adopté la convention de calculer $x_1 \phi_1 x_2 \phi_2 \dots \phi_{k-1} x_k$ de gauche à droite.

- On doit alors justifier que :

$$f(x_1, x_2, \dots, x_{i-1}, x, x_{i+1}, \dots, x_k) = x_1 \phi_1 \dots \phi_{i-1} x \phi_i \dots \phi_{k-1} x_k$$

est une bijection de X sur X , quelles que soient les valeurs prises dans X^{k-1} par $x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_k$ et quel que soit $i \in [1, k]$.

Il suffit pour cela de montrer que tous les types d'équations en x :

$$x_1 \phi_1 x_2 \phi_2 \dots \phi_{i-1} x \phi_{i+1} \dots \phi_{k-1} x_k = b$$
ont une solution et une seule.

Procédons à des changements de variables successifs :

$x_1 \phi_1 x_2 \phi_2 \dots \phi_{k-2} x_{k-1} = Y_1$ permet d'écrire :

$Y_1 \phi_{k-1} x_k = b$, équation ayant une solution et une seule en Y_1 ,

et ainsi de suite, finalement :

$x_1 \phi_1 x_2 \phi_2 \dots \phi_{i-1} x = Y_{k-i}$

Posons : $x_1 \phi_1 x_2 \phi_2 \dots \phi_{i-2} x_i = a$.

L'équation précédente s'écrit :

$$a \phi_{i-1} x = Y_{k-i}$$

et cette équation a une solution et une seule en x . Le résultat est donc acquis et il permet d'obtenir une illustration des arrangements (T_k) à l'aide de structures de quasi-groupes.

REFERENCES.

- [1] - Existence et Propriétés des carrés latins orthogonaux.
Thèse de Mr Guérin.
- [2] - Bruck (R. H.) : Finite Nets II. Uniqueness and Embedding.
Pacific J. Math. 13. (1963), 421-457.
- [3] - Ostrom (T. G.) : Nets with critical deficiency. Pacific.
J. Math. 14 (1964), 1381-1387.
- [4] - Lecoqte Pierre : C.R. Acad. Sc. Paris t. 265 (1967)
p. 196-199.
- [5] - Lecoqte Pierre : C.R. Acad. Sc. Paris t. 265 (1967)
p. 213-215.

C H A P I T R E I I

Application des Réseaux à la construction

de codes correcteurs d'erreurs et de plans d'expériences.

1. Application aux codes correcteurs d'erreurs [réf. 4] .

1) - Les codes correcteurs d'erreurs.

a) Soit X un ensemble fini d'au moins deux éléments désigné par alphabet du code ($\text{Card } [X] = q$).

Soit $\mathcal{E}$ l'ensemble des messages à envoyer.

Soit $f_i, i \in I = [1, N]$, une famille d'applications de $\mathcal{E}$ dans X .

Ces données définiront un code C pourvu que soit réalisé l'axiome de codage suivante :

Axiome de codage.

$$\forall (x, y) \in \mathcal{E}^2, x \neq y, \exists i \in [1, N] \Rightarrow f_i(x) \neq f_i(y)$$

- Soit $V = X^N$. On décrit le code C comme sous-ensemble de V de la façon suivante : à tout $a \in \mathcal{E}$, on fait correspondre l'élément suivant de X^N :

$$[f_1(a), f_2(a), \dots, f_N(a)]$$

Cet élément est souvent désigné comme mot du Code C et N est la longueur des mots du code : $[\mathcal{E}; (f_i; i \in I)]$.

On définit ainsi une application F de $\mathcal{E}$ dans $V = X^N$ et $F(\mathcal{E})$ est la réalisation usuelle d'un code.

b) Un sous-ensemble $J \subset I$ sera un ensemble d'information si $[\mathcal{E}, (f_j; j \in J)]$ définit encore un code et si cela est faux pour tout sous-ensemble de J .

La dimension de $\mathcal{E}$ sera alors définie comme le minimum des cardinaux des ensembles d'information.

S'il y a un ensemble d'information de I de cardinal k et que le cardinal de $\mathcal{E}$ soit égal à q^k , tout ensemble d'information est de cardinal au moins égal à k . C est alors un code (N, k) à k symboles d'information, $N-k$ symboles

de test et de longueur N.

Cette situation est la seule qui sera étudiée dans la suite .

c) Considérons donc un code (N, k) :

$(\mathcal{C} ; f_i , i \in [1, N])$. Soient deux mots a et b de ce code :

$$a \in \mathcal{C} \implies [f_1(a) , f_2(a) , \dots , f_N(a)]$$

$$b \in \mathcal{C} \implies [f_1(b) , f_2(b) , \dots , f_N(b)]$$

Soit alors :

$$d(a , b) = \sum_{i=1}^N \delta_i(a , b)$$

formule dans laquelle on a :

$$\delta_i(a , b) = \begin{cases} 0 & \iff f_i(a) = f_i(b) \\ 1 & \iff f_i(a) \neq f_i(b) \end{cases}$$

Il est facile de vérifier que l'on a ainsi défini une distance (distance de Hamming) et donc une métrique sur X^N .

d) Rappelons les deux propriétés bien connues :

Propriété 1.

Soit le code $F(\mathcal{C}) \subset X^N$ avec la propriété :
 $\forall (x , y) \in [F(\mathcal{C})]^2 , x \neq y , d(x , y) > t , t \text{ fixé},$
 alors il est possible de détecter au plus t erreurs.

Propriété 2.

Soit le code $F(\mathcal{C}) \subset X^N$ avec la propriété :
 $\forall (x , y) \in [F(\mathcal{C})]^2 , x \neq y , d(x , y) > 2t , t \text{ fixé},$
 alors il est possible de corriger au plus t erreurs.

- Si un code $F(\mathcal{C})$ est tel que :

$$\forall (x , y) \in [F(\mathcal{C})]^2 , x \neq y , d(x , y) \geq t , t \text{ fixé},$$

nous dirons par la suite que le code possède la propriété P_t .

Il est bien certain que le code sera d'autant meilleur que pour N et k fixes, t sera plus grand.

Ce sera donc notre objectif en plus de la construction des codes eux-mêmes.

e) Au chapitre IV, nous étudierons des codes, quand l'alphabet peut être muni d'une structure de corps ($X = GF(p^n)$, p premier).

On peut dans ce cas munir le code et X^N d'une norme (dite norme de Hamming).

Sa définition sera la suivante : à tout mot x du code $F(\mathcal{C})$, on peut associer un nombre $\|x\|$ qui est égal au nombre de composantes non nulles de x (si l'on a désigné par 0 l'élément neutre de $GF(p^n)$).

Il est facile de vérifier que l'on a bien ainsi défini une norme et que l'on a :

$$d(x, y) = \|x - y\|, \quad \forall (x, y) \in [F(\mathcal{C})]^2, \quad d(x, y)$$

représentant la distance précédente entre deux mots du code.

Les propriétés 1 et 2 précédentes pourraient alors aussi bien être énoncées en utilisant cette notion de norme.

Il est facile de vérifier qu'un code possédant la propriété P_t est un code dont la norme de tout mot (différent de $(0, 0, \dots, 0)$) est supérieure à t . Il est bien certain enfin que l'on cherchera à construire des codes, qui, pour N et k fixes, ont des mots de norme la plus grande possible.

2) - Construction d'un code à l'aide d'un réseau (R).

Soit un réseau $[E, F, \{F_i\}_{i \in [1, N]}, R, q, k]$

Nous allons lui associer un code de la façon suivante :

Soient f_i , $i = 1, 2, \dots, N$, les applications de E dans F_i qui font correspondre à chaque point de E , le plan de la classe F_i qui passe par x :

$$x \in E \xrightarrow{f_i} y \in F_i$$

Les applications f_i sont, bien entendu, surjectives sans être injectives.

Soit $\mathcal{F} = (f_1, f_2, \dots, f_N)$ l'application correspondante de E dans $F_1 F_2 \dots F_N$:

$$E \xrightarrow{\mathcal{F}} F_1 F_2 \dots F_N$$

Soient ψ_i , $i = 1, 2, \dots, N$ des bijections de F_i sur X ensemble de q éléments et soit $\phi = (\psi_1, \psi_2, \dots, \psi_N)$ l'application correspondante de $F_1 F_2 \dots F_N$ dans X^N :

$$F_1 F_2 \dots F_N \xrightarrow{\phi} X^N$$

Si l'on effectue le produit de $\mathcal{F}$ par ϕ , on fait correspondre à chaque élément de E , un élément de X^N :

$$x \in E \longrightarrow [f_1(x), f_2(x), \dots, f_N(x)] \longrightarrow [\psi_1 f_1(x), \dots, \psi_N f_N(x)]$$

soit en abrégé :

$$E \xrightarrow{\mathcal{F}} F_1 F_2 \dots F_N \xrightarrow{\phi} X^N.$$

On obtient ainsi à partir des points d'un réseau (R) un code :

$$V = \phi \mathcal{F}(E) \subset X^N.$$

a) Vérifions tout d'abord que l'axiome de Codage est bien vérifié.

En effet, d'après la propriété d) de définition des réseaux (R), tous les plans du réseau, appartenant chacun à des classes différentes ne peuvent passer par deux points quelconques. Il existera donc, pour tout couple de points (x_1, x_2) au moins une valeur de $i \in [1, N]$ telle que :

$$\psi_i f_i(x_1) \neq \psi_i f_i(x_2).$$

b) Il est facile de montrer d'autre part que le code ainsi obtenu est un code (N, k) , de longueur N , à k symboles d'information, sur un alphabet de q éléments. On sait en effet (Chapitre I, paragraphe I n°3, 6° propriété) que de tout réseau (R), on peut extraire k classes de plans :

$Fi_1, Fi_2, \dots, Fi_k$ telles que :

$$\forall y^1 \in Fi_1$$

$$\forall y^2 \in Fi_2$$

$$\vdots$$

$$\forall y^k \in Fi_k$$

et pour toute permutation $\alpha(1) \alpha(2) \dots \alpha(k)$ de $(1, 2, \dots, k)$ l'on ait :

$$\text{Card} [y^{\alpha(1)} \cap y^{\alpha(2)} \cap y^{\alpha(3)}] = q^{k-3}$$

...

$$\text{Card} [y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(h)}] = q^{k-h}$$

...

$$\text{Card} [y^{\alpha(1)} \cap y^{\alpha(2)} \cap \dots \cap y^{\alpha(k)}] = 1$$

Donc, si à tout point x de E on fait correspondre

$$[f_{i_1} \psi_{i_1}(x), f_{i_2} \psi_{i_2}(x), \dots, f_{i_k} \psi_{i_k}(x)] ,$$

on obtient encore un code mais on ne peut le raccourcir davantage, car alors l'axiome de codage ne serait plus rempli.

On a donc bien k symboles d'information.

3) - Codes associés à des réseaux $(R)_{k-1}$ et des réseaux $(R)_t$.

a) Code associé à un réseau $(R)_{k-1}$.

En utilisant les résultats du chapitre I et en particulier les théorèmes 1 et 2 du paragraphe II, on voit que l'on peut associer à un réseau $(R)_{k-1}$, un code :

$$[x_1, x_2, \dots, x_k, a^1, a^2, \dots, a^h]$$

formule dans laquelle, rappelons-le :

$$x_i \in X \quad , \quad \forall i \in [1, k]$$

$$a^j = f_j(x_1, x_2, \dots, x_k) \quad , \quad \forall j \in [1, h] .$$

On obtient donc dans ce cas un code de longueur $k+h$

à k symboles d'information $x_1, x_2, \dots, x_k$ (les symboles de test étant $a^1, a^2, \dots, a^h$) sur un ensemble X de q éléments.

Ce code possède la propriété P_{h+1} d'autre part. En effet, par tout couple de points (x_1, x_2) du réseau ne passent pas plus de $k-1$ plans et par conséquent :

$$d[\phi \mathcal{F}(x_1), \phi \mathcal{F}(x_2)] \geq h+1$$

Dans ce cas particulier, le code sera optimum, si h est maximisé. On dira alors que la famille d'arrangements orthogonaux (T_k) correspondante est complète.

b) Code associé à un réseau $(\hat{R})_{h+k-t-1}$

On utilise les résultats du théorème 3 du paragraphe II du chapitre I.

A un réseau $(\hat{R})_{h+k-t-1}$ correspond donc un code $(h+k, k)$ décrit par :

$$\begin{aligned} &[x_1, x_2, \dots, x_k, a^1, a^2, \dots, a^h] \\ &x_i \in X, \quad \forall i \in [1, k] \\ &a^j = f_j(x_1, x_2, \dots, x_k), \quad \forall j \in [1, h] \end{aligned}$$

Ce code possède la propriété P_{t+1} puisqu'alors :

$$\forall (x_1, x_2) \in E^2, x_1 \neq x_2, d[\phi \mathcal{F}(x_1); \phi \mathcal{F}(x_2)] \geq t+1$$

Le code est alors optimum, si h et k étant fixés, le réseau $(\hat{R})_{h+k-t-1}$ a été construit de façon à ce que t soit maximum.

II. Application des Réseaux à la construction de Plans en Blocs Incomplets.

1) - Rappels de quelques définitions (réf. [2])

Soient $E = \{e_j\}$, $j = 1, 2, \dots, v$ un ensemble de v éléments ou variétés et $B_1, B_2, \dots, B_b$, b parties de E ou blocs. On désigne par "plan en blocs incomplets" l'ensemble formé par $B_1, B_2, \dots, B_b$.

On peut distinguer deux classes de plans en blocs incomplets (on étudiera une troisième classe au paragraphe suivant) particulièrement étudiées :

a) Les plans en blocs égaux incomplets équilibrés.

Ce sont des plans en blocs incomplets jouissant des propriétés suivantes :

$$- \text{Card } [B_i] = k, \quad \forall i \in [1, b].$$

(Chaque bloc contient k variétés).

$$- \sum_{i=1}^b \text{Card} [\{x\} \cap B_i] = r, \quad \forall x \in E$$

(Chaque variété apparaît dans r blocs).

$$- \sum_{i=1}^b \text{Card} [\{x, y\} \cap B_i] = \lambda, \quad \forall (x, y) \in E^2, \quad x \neq y.$$

(Chaque couple de variétés se trouve dans λ blocs).

b) Les Plans en blocs égaux partiellement équilibrés.

On définit sur E une "relation d'association" (ou "schéma d'association") :

Si $R_1, R_2, \dots, R_m$ sont m relations binaires symétriques et si $\forall (x, y) \in E$, il existe i unique tel que :

$x R_i y$, on dit que x et y sont $i^{\text{èmes}}$ associées. On désigne par A_j^x l'ensemble des éléments de E (ou variétés du plan), $j^{\text{ième}}$ associés de x. Un plan en blocs égaux partiellement équilibrés est un plan en blocs incomplets où l'on a défini une relation d'association entre les variétés et tels que :

$$- \text{Card } [B_i] = k, \quad \forall i \in [1, b]$$

$$- \sum_{i=1}^b \text{Card} [\{x\} \cap B_i] = r, \quad \forall x \in E$$

$$- \sum_{i=1}^b \text{Card} [\{x, y\} \cap B_i] = \lambda_j, \quad \begin{cases} \forall x \neq y \in E \\ y \in A_j^x \end{cases}$$

$$- \text{Card } [A_j^x] = n_j, \quad \forall x \in E$$

$$- \text{Card} [A_j^x \cap A_k^y] = p_{jk}^i, \quad \begin{cases} \forall x, y \in E \\ y \in A_i^x \end{cases}$$

Les paramètres n_j sont dits de première espèce.

Les paramètres p_{jk}^i sont dits de seconde espèce.

2) - Construction de plans en blocs incomplets.

a) Construction.

Soit un réseau (R) de dimension k :

$(E, F, F_i, i \in [1, N], R, q, k)$. On peut lui faire correspondre un plan en blocs incomplets de la façon suivante :

- Les variétés sont les points du réseau.

Donc : $v = q^k$.

- Les blocs sont les plans du réseau.

Donc : $b = q^N$.

b) Propriétés du plan en blocs incomplets, construit

- $\text{Card } [B_i] = q^{k-1}$.

On a donc un plan en blocs égaux.

- D'après les propriétés de définition des réseaux (R) de dimension k, on sait que par tout point, il passe un plan et un seul de chaque classe de plans : ce qui se traduit ici par le fait que toute variété appartient exactement à N blocs.

$$r = \sum_{i=1}^b \text{Card } [\{x\} \cap B_i] = N$$

Relation d'association.

On peut introduire la relation d'association suivante entre les variétés :

Deux variétés sont $i^{\text{ièmes}}$ associées si et seulement s'il passe i blocs par ces deux variétés.

(Le langage correspondant dans les réseaux est le suivant : deux points sont $i^{\text{èmes}}$ associés si et seulement s'il passe i plans par ces deux points).

Si le réseau (R) est un réseau $(R)_t$, on a ainsi (t+1) possibilités : $i = 0, 1, 2, \dots, t$.

La relation d'association ainsi définie n'est pas

en général celle d'un plan en blocs partiellement équilibrés comme nous allons le voir (dans le cas particulier $k = 2$, on obtient un plan en blocs partiellement équilibrés (référence [2])).

Nous distinguerons deux cas suivant que $t = k-1$ ou que $t \neq k-1$.

$\alpha)$ Cas des réseaux $(R)_{k-1}$.

A - Calcul de la valeur des paramètres de 1^o espèce.

Soit n_j le nombre de $j^{\text{èmes}}$ associés d'une variété x quelconque. ($j = 0, 1, 2, \dots, k-1$).

Reportons-nous au réseau à partir duquel on a construit le plan en blocs incomplets considéré.

C'est par hypothèse un réseau $(R)_{k-1}$ de dimension k :

$$(E, F, F_i, i \in [1, N], R, q, k).$$

Dans ces conditions $n_j(x)$, qui doit avoir une valeur indépendante du point x choisi, désigne le nombre de points du réseau $(R)_{k-1}$ par lesquels, il passe exactement j plans, passant déjà par x ($\forall j \in [0, k-1]$).

Ainsi que nous allons le vérifier n_j dépend de façon très particulière des valeurs de N et de k . Aussi poserons-nous :

$$n_j = n_j [N, k], \quad \forall j \in [0, k-1]$$

Le calcul de $n_j [N, k]$ repose alors sur une propriété des réseaux $(R)_{k-1} : (E, F, F_i, i \in [1, N], R, q, k) :$

Propriété.

(1) - Soit un réseau $(R)_{k-1} :$

$(E, F, F_i, i \in [1, N], R, q, k)$. Un plan quelconque de ce réseau peut être considéré comme un réseau $(R)_{k-2} :$
 $(E', F', F'_{i'}, i' \in [1, N-1], R', q, k-1).$

(2) - Plus généralement l'intersection de h plans quelconques de h classes différentes du réseau $(R)_{k-1}$

peut être considéré comme un réseau $(R)_{k-h-1}$:

$$(E'' , F'' , F''_{i''} , i'' \in [1, N-h] , R'' , q , k-h).$$

Démonstration.

(I) - Soit y le plan quelconque du réseau $(R)_{k-1}$.

- Les points du réseau $(R)_{k-2}$ correspondant seront les points de y : $E' = y$.

- Les plans du réseau $(R)_{k-2}$ correspondant seront les intersections des plans du réseau primitif avec y :

$$F' = \{ z \cap y : \forall z \in F \} .$$

On obtient donc $N-1$ classes de plans (la classe des plans parallèles à y saute bien entendu).

Il est facile de vérifier ensuite sur E' et F' ainsi construits les propriétés d'un réseau $(R)_{k-2}$ de dimension $k-1$.

(II) - La deuxième partie de la propriété suit par répétition du procédé de construction précédent h fois :

- $E'' = y_1 \cap y_2 \cap \dots \cap y_h$ (si $y_1, y_2, \dots, y_h$ sont les h plans de $(R)_{k-1}$ choisis).

$$- F'' = \{ z \cap y_1 \cap y_2 \cap \dots \cap y_h : \forall z \in F \} .$$

On obtient donc $N-h$ classes de plans (les h classes de plans auxquelles appartiennent $y_1, y_2, \dots, y_h$ sautent bien entendu).

On peut maintenant calculer $n_j [N, k]$.

Démontrons tout d'abord la relation :

$$(1). \quad n_j [N, k] = C_N^j n_0 [N-j, k-j] , \quad \forall j \in [0, k-1]$$

Par tout point x du réseau $(R)_{k-1}$, il passe N plans. Il y a d'autre part C_N^j façons différentes de choisir j plans parmi ces N plans ; chacune d'elles donne des points $j^{\text{èmes}}$ associés du point x pourvu que par ces points, il ne passe pas d'autres plans d'où la relation (1) indiquée (en utilisant la propriété démontrée précédemment : les j plans s'intersectent

suivant un réseau $(R)_{k-j-1}$ de dimension $k-j$).

On ramène ainsi le calcul de $n_j [N, k]$ au calcul de $n_0 [N, k]$.

Démontrons maintenant la relation :

$$(2). \quad n_0 [N, k] = (q^k - 1) - \sum_{i=1}^{k-1} C_N^i n_0 [N-i, k-i]$$

Cette égalité est en fait une identité comptable : elle exprime que $n_0 [N, k]$ est égal au nombre de points du réseau différents de x (soit $q^k - 1$), nombre duquel on a retiré :

- le nombre de points par lesquels il passe un plan passant déjà par x , soit $C_N^1 n_0 [N-1, k-1]$

- le nombre de points par lesquels il passe deux plans passant déjà par x , soit $C_N^2 n_0 [N-2, k-2]$

- ...

- le nombre de points par lesquels il passe $k-1$ plans passant déjà par x , soit $C_N^{k-1} n_0 [N-k+1, 1]$.

Nous allons voir enfin, par récurrence sur k que :

$$n_0 [N, k] = \sum_{h=0}^{k-1} (-1)^h C_N^h (q^{k-h} - 1)$$

Cette relation est en effet vérifiée pour $k=2$. Supposons-la exacte jusqu'à l'ordre $k-1$ et utilisons la relation (2).

On a :

$$n_0 (N, k) = (q^k - 1) - \sum_{i=1}^{k-1} C_N^i n_0 [N-i, k-i]$$

Or :

$$n_0 (N-i, k-i) = \sum_{h_1=0}^{k-i-1} (-1)^{h_1} C_{N-i}^{h_1} (q^{k-i-h_1} - 1)$$

(en utilisant l'hypothèse de récurrence).

On a donc :

$$n_0 (N, k) = (q^k - 1) - \sum_{i=1}^{k-1} \left[\sum_{h_1=0}^{k-i-1} C_N^i (-1)^{h_1} C_{N-i}^{h_1} (q^{k-i-h_1} - 1) \right]$$

Posons : $s = i + h_1$

On a :

$$C_N^i C_{N-i}^{h_1} = C_s^i C_N^s$$

et :

$$n_o(N, k) = (q^{k-1}) - \sum_{i=1}^{k-1} \sum_{s=i}^{k-1} C_s^i C_N^s (-1)^{s-i} (q^{k-s-1})$$

Ce qui peut encore s'écrire :

$$n_o(N, k) = (q^{k-1}) - \sum_{s=1}^{k-1} \left[\sum_{i=1}^s C_s^i C_N^s (-1)^{s-i} (q^{k-s-1}) \right]$$

Soit :

$$n_o(N, k) = (q^{k-1}) - \sum_{s=1}^{k-1} C_N^s (-1)^s (q^{k-s-1}) \left[\sum_{i=1}^s (-1)^i C_s^i \right]$$

Or :

$$\sum_{i=1}^s (-1)^i C_s^i = -1$$

Donc :

$$n_o(N, k) = \sum_{s=0}^{k-1} (-1)^s C_N^s (q^{k-s-1})$$

Et la formule proposée est donc établie par récurrence.

Utilisons alors la relation (1), il vient :

$$n_j[N, k] = C_N^j n_o[N-j, k-j]$$

et on obtient :

$$n_j(N, k) = C_N^j \sum_{h=0}^{k-j-1} (-1)^h C_{N-j}^h (q^{k-j-h-1})$$

formule pouvant encore s'écrire :

$$n_j(N, k) = \sum_{h=0}^{k-j-1} (-1)^h C_N^h C_{N-h}^j (q^{k-j-h-1})$$

$$\underline{j = 0, 1, 2, \dots, k-1.}$$

B - Le calcul de la valeur des paramètres de seconde espèce p_j^i k dépend a priori du couple de variétés $i^{\text{èmes}}$ associées choisies (x, y) . $((x, y) \in E^2, x \neq y)$.

Nous allons le vérifier dans un cas particulier, ce qui nous permettra de constater que le schéma d'association des plans d'expériences construits n'est pas celui d'un plan en blocs partiellement équilibrés.

Cas particulier.

Lorsque $q = p^n$, p étant un nombre premier, l'ensemble X (défini au Chapitre I) peut être muni d'une structure de Corps de Galois $GF(q)$.

Si l'on considère alors la géométrie Euclidienne à k dimensions $EG [q ; k]$, on peut en extraire un réseau $(R)_{k-1}$ de dimension k de la façon suivante :

(i). Les points du réseau $(R)_{k-1}$ seront identiques aux points de la Géométrie Euclidienne $(x_1, x_2, \dots, x_k)$, $x_i \in GF(q)$, $\forall i \in [1, k]$.

(ii). Les N classes de q plans du réseau $(R)_{k-1}$ sont extraites des plans de la Géométrie Euclidienne choisie, ainsi :

- k classes sont de la forme :

$$\left\{ \begin{array}{l} 1^{\text{e}} \text{ classe : } x_1 = \alpha_1, \quad \forall \alpha_1 \in GF(q) \\ 2^{\text{e}} \text{ classe : } x_2 = \alpha_2, \quad \forall \alpha_2 \in GF(q) \\ \vdots \\ k^{\text{ème}} \text{ classe : } x_k = \alpha_k, \quad \forall \alpha_k \in GF(q). \end{array} \right.$$

- $(N-k)$ classes ont pour équations :

$$\left\{ \begin{array}{l} (k+1)^{\text{ème}} \text{ classe : } \sum_{j=1}^k a_{1,j} x_j = \beta_1, \quad \forall \beta_1 \in GF(q) \\ (k+2)^{\text{ème}} \text{ classe : } \sum_{j=1}^k a_{2,j} x_j = \beta_2, \quad \forall \beta_2 \in GF(q) \\ \vdots \\ N^{\text{ème}} \text{ classe : } \sum_{j=1}^k a_{N-k,j} x_j = \beta_{N-k}, \quad \forall \beta_{N-k} \in GF(q). \end{array} \right.$$

Les a_{ij} sont des éléments fixes de $GF(q)$ et l'on a un réseau $(R)_{k-1}$ si la matrice (a_{ij}) de $N-k$ lignes et k colonnes correspondantes est telle que toutes les sous-matrices que l'on puisse en extraire soient régulières (ce qui nécessite en particulier que tous les éléments a_{ij} soient différents de l'élément neutre du corps $GF(q)$).

Supposons donc que l'on ait construit un réseau $(R)_{k-1}$ de cette façon.

On sait que l'on peut prolonger la géométrie Euclidienne $EG [q ; k]$ de départ en une géométrie projective à k dimensions, soit $PG [q ; k]$.

La géométrie euclidienne $EG [q ; k]$ s'obtient alors à partir de la géométrie projective $PG [q ; k]$ en otant de cette géométrie un hyperplan, soit une géométrie projective à $k-1$ dimensions : $PG [q ; k-1]$.

Au réseau $(R)_{k-1}$ précédent correspond alors dans cette géométrie projective $PG [q ; k-1]$:

- les points de cette géométrie $(x_1, x_2, \dots, x_k)$ (en coordonnées homogènes).
- les plans suivants de cette géométrie :

$$\left\{ \begin{array}{l} 1^\circ \text{ plan : } x_1 = 0 \\ 2^\circ \text{ plan : } x_2 = 0 \\ \vdots \\ k^\circ \text{ plan : } x_k = 0 \\ (k+1)^\circ \text{ plan : } \sum_{j=1}^k a_{1,j} x_j = 0 \\ (k+2)^\circ \text{ plan : } \sum_{j=1}^k a_{2,j} x_j = 0 \\ \vdots \\ N^\circ \text{ plan : } \sum_{j=1}^k a_{N-k,j} x_j = 0 \end{array} \right.$$

(en désignant l'élément neutre du corps par 0).

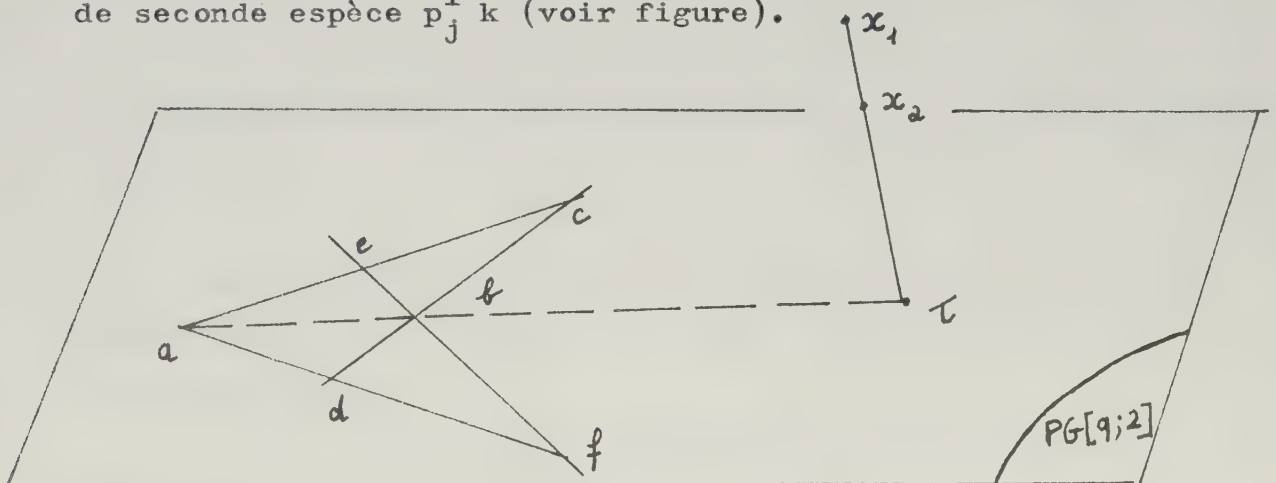
On obtient donc N plans qui doivent posséder la propriété suivante (correspondant à la propriété de la matrice (a_{ij})) :

Par tout point de la géométrie projective $PG [q ; k-1]$, il ne passe pas plus de $k-1$ plans (pris parmi les N précédents). Dans ce cas particulier, on voit donc que le problème de la construction d'un réseau $(R)_{k-1}$ est remplacé par le problème suivant :

Construire dans une géométrie projective à $k-1$ dimensions $PG [q ; k-1]$ une famille d'hyperplans telle que par tout point de cette géométrie, il ne passe pas plus de $k-1$ hyperplans.

On peut donc dans ce cas associer à un réseau $(R)_{k-1}$ une géométrie projective à $k-1$ dimensions et une famille d'hyperplans dans cette géométrie possédant la propriété indiquée précédemment.

Prenons pour fixer les idées le cas d'un réseau $(R)_{k-1}$ avec $k = 3$ et $N = 4$; calculons alors les paramètres de seconde espèce $p_j^i k$ (voir figure).



Soient x_1 et x_2 deux points du réseau. Supposons que la droite $x_1 x_2$ rencontre la géométrie projective $PG [q ; 2]$ associée en τ , les quatre classes de plans du réseau ayant pour correspondants dans cette géométrie : les droites (ac) , (af) , (ef) , et (c,d) . Si le point τ est aligné avec les points a , b (ou bien avec les points (e,d) ou (c,f)), $p_{2,2}^0(x_1, x_2)$ ne sera pas nulle ($a x_1$ et $b x_2$ se couperont en un point,

a x_2 et b x_1 également, d'où : $p_{2,2}^0(x_1, x_2) = 2$). Si par contre le point $\bar{c}$ n'est pas aligné avec les points (a,b) ou (e,d) ou (c,f), il est bien évident géométriquement que $p_{2,2}^0(x_1, x_2) = 0$.

p_j^i dépend donc du couple de points choisi et le plan d'expériences construit n'est donc pas un plan en blocs partiellement équilibrés.

β) Cas des réseaux $(R)_t$.

Les remarques précédentes se transposent aisément au cas général des réseaux $(R)_t$.

On doit cependant ajouter que le calcul des paramètres de première espèce n'est possible que si la structure combinatoire de ces réseaux est entièrement précisée, ce qui peut poser de sérieux problèmes de calculs.

C - Nous allons revenir dans le paragraphe suivant sur l'étude de ces plans incomplets et voir qu'aux réseaux $(R)_{k-1}$ s'adaptent très facilement des structures de tableaux orthogonaux.

III. Applications des réseaux à la construction de Plans en blocs Incomplets (suite). Le cas des Tableaux orthogonaux [référence 1].

1) - Définition d'un tableau orthogonal.

Soit (a_{ij}) une matrice de N lignes et M colonnes dont les éléments sont pris dans un ensemble X de q éléments.

Soit (P) la propriété suivante :

Toute sous-matrice de k lignes, M colonnes, extraite de la matrice (a_{ij}) est telle que tous les k-tuples qu'il est possible de former à l'aide des éléments de X soient représentés chacun à λ exemplaires par les colonnes de la sous-matrice (k, M). Une matrice (a_{ij}) possédant la propriété (P) est

appelée tableau orthogonal de force k possédant N contraintes, d'indice λ . On désigne ce tableau orthogonal par ses caractéristiques : (λ, N, q, k) .

On a bien sûr la relation :

$$M = \lambda q^k.$$

2) - Construction d'un tableau orthogonal.

Théorème.

L'existence d'un réseau $(R)_{k-1}$ de dimension k , de q^k points et de N classes de q plans parallèles entraîne l'existence d'un tableau orthogonal dont les caractéristiques sont : $(1, N, q, k)$ et réciproquement.

Démonstration.

On a déjà montré qu'à un réseau $(R)_{k-1}$ de dimension k correspondaient $N-k$ arrangements (T_k) orthogonaux, soient :

$$(x_1, x_2, \dots, x_k ; a_1, a_2, \dots, a_{N-k})$$

$$x_i \in X, \quad \forall i \in [1, k],$$

$$a_j = f_j(x_1, x_2, \dots, x_k), \quad \forall j \in [1, N-k]$$

Le tableau orthogonal correspondant sera décrit en faisant varier $x_1, x_2, \dots, x_k$ dans X et en écrivant chaque N -tuples $(x_1, x_2, \dots, x_k ; a_1, a_2, \dots, a_{N-k})$ en colonne.

	x_1	
	x_2	
	$\vdots$	
	x_k	
	a_1	
	a_2	
	$\vdots$	
	a_{N-k}	

Il est facile de vérifier que l'on a bien obtenu un tableau orthogonal, en appliquant les propriétés des arrangements (T_k) orthogonaux. Extrayons, en effet, du tableau, une matrice

de k lignes et q^k colonnes en prenant par exemple i lignes parmi les k premières et les $k-i$ autres lignes parmi les $h = N-k$ dernières.

Cette matrice correspond au cas où l'on considère un système de $k-i$ équations à $k-i$ inconnues, système qui n'a qu'une seule solution.

Si l'on examine alors deux colonnes de cette matrice telles que :

$$(x_{j_1}, x_{j_2}, \dots, x_{j_i}) = (x'_{j_1}, x'_{j_2}, \dots, x'_{j_i})$$

on aura :

$$(a_{h_1}, a_{h_2}, \dots, a_{h_{k-i}}) \neq (a'_{h_1}, a'_{h_2}, \dots, a'_{h_{k-i}})$$

Sinon le système de $k-i$ inconnues et de $k-i$ équations correspondant aurait deux solutions.

De même :

$$(a_{h_1}, a_{h_2}, \dots, a_{h_{k-i}}) = (a'_{h_1}, a'_{h_2}, \dots, a'_{h_{k-i}})$$

entraîne :

$$(x_{j_1}, x_{j_2}, \dots, x_{j_i}) \neq (x'_{j_1}, x'_{j_2}, \dots, x'_{j_i})$$

pour la même raison.

Réciproquement, soit un tableau orthogonal dont les caractéristiques sont $(1, N, q, k)$. Dans toute sous-matrice de la matrice $(N \times q^k)$ définissant le tableau orthogonal, de k lignes et de q^k colonnes chaque k -tuple que l'on peut former à l'aide des éléments de X est représenté une fois et une seule.

Considérons une colonne quelconque. Désignons les k premiers éléments par $x_1, x_2, \dots, x_k$, les $h = N-k$ derniers par $f_1(x_1, x_2, \dots, x_k), f_2(x_1, x_2, \dots, x_k), \dots, f_h(x_1, x_2, \dots, x_k)$.

On a ainsi construit h arrangements orthogonaux (T_k) ($N-k = h$) : $(x_1, x_2, \dots, x_k; f_i(x_1, x_2, \dots, x_k))$

Effectivement, vérifions tout d'abord que l'on a des arrangements (T_k) .

Prenons par exemple les $k-1$ premières lignes et la $k+i$ ème ligne. Il s'agit alors de vérifier que :

$$f_i(x_1, x_2, \dots, x_{k-1}, X) = a_i$$

a une solution et une seule en X . Effectivement, si cette équation avait deux solutions X_1 et X_2 , le k -tuple $(x_1, x_2, \dots, x_{k-1}, a_i)$ apparaîtrait deux fois, ce qui n'est pas possible. On a donc bien des arrangements (T_k) et il est immédiat de constater que ce sont des arrangements orthogonaux en considérant $k-i$ lignes parmi les k premières et i lignes parmi les $h = N-k$ dernières.

c. q. f. d.

IV. Application à la construction des ovales [réf. 3]

1) - Définition des ovales.

La construction des ovales a tout d'abord été envisagée dans un plan projectif.

Il s'agissait de construire une famille de points dans une Géométrie Projective à deux dimensions telle que :

- a) - trois points quelconques de la famille ne soient pas alignés.
 - b) - Il ne soit pas possible d'ajouter à la famille un point restant de la géométrie et de conserver la propriété a).
- On désignait par "ovale" une famille de points possédant les propriétés a) et b).

Le problème de construction conduit naturellement à chercher le nombre maximum de points non alignés d'une géométrie projective à deux dimensions.

La famille de points ainsi construite sera un ovale. On peut bien entendu s'intéresser au problème correspondant dans le cas général d'une Géométrie Projective à k dimensions.

Il s'agira de chercher le nombre maximum de points d'une PG $[k ; q]$ tels que $k+1$ quelconques d'entre eux n'appartiennent pas à un même hyperplan.

La famille de points ainsi construite constituera un "ovale".

2) - Equivalence avec certains réseaux $(R)_{k-1}$.

Nous avons vu au paragraphe II de ce chapitre que lorsque les réseaux $(R)_{k-1}$ sont des familles d'hyperplans extraits d'une Géométrie Euclidienne à k dimensions, le problème de leur construction revient à chercher des familles d'hyperplans extraites d'une PG $[k-1, q]$ telles que par tout point de la géométrie ne passent pas plus de $k-1$ hyperplans.

Le Problème dual consistera à construire une famille de points tels que sur tout hyperplan de la géométrie, il n'y ait pas plus de $k-1$ points de la famille. Autrement dit, par k points quelconques de la famille ne passent aucun hyperplan de la géométrie.

La recherche des réseaux $(R)_{k-1}$ "complets" c'est-à-dire la recherche du nombre maximum d'hyperplans tels que par tout point il ne passe pas plus de $k-1$ hyperplans est donc équivalente à la recherche d'un ovale par dualité.

REFERENCES.
=====

- [1] - I.M. Chakravarti. Séminaire de l'Institut de Statistique du 9 Avril 1962 sur les tableaux orthogonaux.
- [2] - R. Guérin. Vue d'ensemble sur les plans en blocs incomplets équilibrés et partiellement équilibrés. Institut International de Statistique. 34^e Session. Ottawa. 1963.
- [3] - B. Segre. Lectures on modern geometry. 7. Edizioni Cremonese. Roma. 1961.
- [4] - Peterson. Error correcting Codes. Wiley. 1961.

C H A P I T R E I I I

Construction de réseaux (R).

Ce chapitre est particulièrement consacré à la construction de réseaux $(R)_{k-1}$.

Ainsi la généralisation de la construction des carrés latins mutuellement orthogonaux par produit direct ([1]), la généralisation de la notion de transversales ([1] et [2]), la généralisation de la notion d'isotopie ([1] et [6]) sont des paragraphes intéressants uniquement le cas des réseaux $(R)_{k-1}$. Nous donnerons ensuite des exemples simples de construction de réseaux (R) , surtout dans le cas où l'ensemble X peut être muni d'une structure de Corps de Galois.

I. Construction de Réseaux $(R)_{k-1}$ par produit direct.

La construction des réseaux par produit direct généralise celle des quasi-groupes mutuellement orthogonaux par le même procédé. Nous commencerons donc ce paragraphe par le rappel de cette construction.

1) - Construction de quasi-groupes mutuellement orthogonaux par produit direct.

Soit E un ensemble de q_1 éléments. Soient ϕ_1 et ϕ'_1 deux lois munissant E de structures de quasi-groupes orthogonales. Soit un ensemble F de q_2 éléments. Soient ϕ_2 et ϕ'_2 deux lois munissant F de structures de quasi-groupes orthogonales.

On définit alors sur $G = E \times F$ deux lois ψ et ψ' de la façon suivante :

$$(x, x') \psi (y, y') = (x \phi_1 y, x' \phi_2 y')$$

$$(x, x') \psi' (y, y') = (x \phi'_1 y, x' \phi'_2 y')$$

$$\forall (x, y) \in E^2$$

$$\forall (x', y') \in F^2$$

Théorème 1. Les lois ψ et ψ' munissent G de structures de quasi-groupes orthogonales.

Démonstration.

a) On peut montrer que ψ par exemple munit G d'une structure de quasi-groupe. (Ce sera la même chose pour ψ'). C'est-à-dire que :

$$X \psi X' = X \psi X'' \implies X' = X'' \quad \forall X \in G.$$

En effet :

$$(x, x') \psi (y, y') = (x, x') \psi (z, z')$$

s'écrit :

$$(x \phi_1 y) , x' \phi_2 y') = (x \phi_1 z , x' \phi_2 z')$$

Donc :

$$x \phi_1 y = x \phi_1 z$$

ce qui entraîne : $y = z$

et :

$$x' \phi_2 y' = x' \phi_2 z'$$

ce qui entraîne : $y' = z'$.

On démontrerait de même que :

$$X' \psi X = X'' \psi X \implies X' = X'' \quad \forall X \in G$$

b) On doit montrer ensuite que :

$$\begin{cases} X \psi Y = X' \psi Y' \\ X \psi' Y = X' \psi' Y' \end{cases}$$

entraîne :

$$\begin{cases} X = X' \\ Y = Y' \end{cases}$$

En effet, le système :

$$\begin{cases} (x, x') \psi (y, y') = (z, z') \psi (t, t') \\ (x, x') \psi' (y, y') = (z, z') \psi' (t, t') \end{cases}$$

peut s'écrire :

$$\begin{aligned} (x \phi_1 y , x' \phi_2 y') &= (z \phi_1 t , z' \phi_2 t') \\ (x \phi'_1 y , x' \phi'_2 y') &= (z \phi'_1 t , z' \phi'_2 t'). \end{aligned}$$

D'où :

$$\begin{cases} x \phi_1 y = z \phi_1 t \\ x \phi'_1 y = z \phi'_1 t \end{cases}$$

et :

$$\begin{cases} x' \phi_2 y' = z' \phi_2 t' \\ x' \phi'_2 y' = z' \phi'_2 t' \end{cases}$$

qui entraînent, vues les hypothèses :

$$\begin{cases} x = z \\ y = t \end{cases}$$

$$\begin{cases} x' = z' \\ y' = t' \end{cases}$$

soit : $(x, x') = (z, z')$

et : $(y, y') = (t, t')$

2) - Construction de Réseaux par produit direct.

a) Soient d'une part, un ensemble E, Card $[E] = p$ et n arrangements (T_k) orthogonaux sur E :

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)] \quad , i \in [1, n]$$

Soient d'autre part, un ensemble F, Card $[F] = q$ et m arrangements (T_k) orthogonaux sur F :

$$[y_1, y_2, \dots, y_k ; g_j(y_1, y_2, \dots, y_k)] \quad , j \in [1, m]$$

On définit alors sur $G = E \times F$, min $[n, m]$ arrangements (T_k) de la façon suivante :

$$[(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k) ; (f_i(x_1, x_2, \dots, x_k), g_i(y_1, y_2, \dots, y_k))] \quad i = 1, 2, \dots, \min [n, m]$$

On peut alors énoncer le théorème suivant :

Théorème 2. Les familles d'arrangements (T_k) ainsi construites sur G, forment des familles de min $[n, m]$ arrangements (T_k) orthogonaux.

Démonstration.

Posons :

$$a^i = f_i(x_1, x_2, \dots, x_k)$$

$$b^i = g_i(y_1, y_2, \dots, y_k)$$

$$X_i = (x_i, y_i) \quad \forall i \in [1, k]$$

$$A_i = (a^i, b^i) \quad \forall i \in [1, \min(n, m) = h]$$

On aura une famille de h arrangements (T_k) orthogonaux sur G :

$$[X_1, X_2, \dots, X_k; A_i], \quad i \in [1, h]$$

si et seulement si le système I suivant a la propriété suivante :

Tout système de α équations à α inconnues tiré de I a une solution et une seule ($1 \leq \alpha \leq \min [h, k]$).

$$I \quad \begin{cases} A^1 = F_1(X_1, X_2, \dots, X_k) \\ A^2 = F_2(X_1, X_2, \dots, X_k) \\ \vdots \\ A^h = F_h(X_1, X_2, \dots, X_k) \end{cases}$$

(On a posé $F_i(X_1, X_2, \dots, X_k) = [f_i(x_1, x_2, \dots, x_k), g_i(y_1, y_2, \dots, y_k)] \quad \forall i \in [1, h]$).

Nous prouverons ainsi en même temps (pour $\alpha = 1$) que l'on a bien des arrangements (T_k) sur G , ce qui demandait à être justifié également.

Le système I peut s'écrire de la façon suivante :

$$\begin{cases} (a^i, b^i) = F_i [(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)] \\ i \in [1, h] \end{cases}$$

c'est-à-dire :

$$\begin{cases} (a^i, b^i) = [f_i(x_1, x_2, \dots, x_k), g_i(y_1, y_2, \dots, y_k)] \\ i \in [1, h] \end{cases}$$

Donc :

$$\begin{cases} a^i = f_i(x_1, x_2, \dots, x_k) & (1) \\ i \in [1, h] \\ b^i = g_i(y_1, y_2, \dots, y_k) & (2) \\ i \in [1, h] \end{cases}$$

Un système de α équations $i_1, i_2, \dots, i_\alpha$ à α inconnues : $X_{j_1}, X_{j_2}, \dots, X_{j_\alpha}$ extrait du système I se traduit donc par deux systèmes :

- un système de α équations : $i_1, i_2, \dots, i_\alpha$ à α inconnues $x_{j_1}, x_{j_2}, \dots, x_{j_\alpha}$ extrait de (1) :

$$\begin{cases} a^{i_1} = f_{i_1}(x_1, x_2, \dots, x_k) \\ a^{i_2} = f_{i_2}(x_1, x_2, \dots, x_k) \\ \vdots \\ a^{i_\alpha} = f_{i_\alpha}(x_1, x_2, \dots, x_k) \end{cases}$$

- un système de α équations $i_1, i_2, \dots, i_\alpha$ à α inconnues $y_{j_1}, y_{j_2}, \dots, y_{j_\alpha}$ extrait de (2).

$$\begin{cases} b^{i_1} = g_{i_1}(y_1, y_2, \dots, y_k) \\ b^{i_2} = g_{i_2}(y_1, y_2, \dots, y_k) \\ \vdots \\ b^{i_\alpha} = g_{i_\alpha}(y_1, y_2, \dots, y_k) \end{cases}$$

Chacun de ces deux systèmes admet par hypothèse une solution et une seule :

$$(x_{j_1}^*, x_{j_2}^*, \dots, x_{j_\alpha}^*) \quad \text{et} \quad (y_{j_1}^*, y_{j_2}^*, \dots, y_{j_\alpha}^*)$$

$$\forall \alpha \in [1, \min(h, k)] .$$

En posant : $X_i^* = (x_i^*, y_i^*)$, on voit donc que le système primitif I admet une solution et une seule :

$$(X_{j_1}^*, X_{j_2}^*, \dots, X_{j_\alpha}^*) , \quad \forall \alpha \in [1, \min [h, k]]$$

c. q. f. d.

- L'équivalence entre réseaux $(R)_{k-1}$ et familles d'arrangements (T_k) orthogonaux permet d'énoncer le corollaire suivant :

Corollaire 1.

L'existence de deux réseaux $(R)_{k-1}$:

$$[E_1, F_1, F_{1,i}, i \in [1, 2, \dots, N_1+k], R_1, q_1, k]$$

$$[E_2, F_2, F_{2,j}, j \in [1, 2, \dots, N_2+k], R_2, q_2, k]$$

entraîne l'existence d'un réseau $(R)_{k-1}$:

$$[E_1 \times E_2, F, F_i, i \in [1, 2, \dots, k + \min [N_1, N_2]], R, q_1 q_2, k]$$

b) Généralisation du procédé.

Soient h ensembles E_i , $\text{Card}[E_i] = p_i$, $i \in [1, h]$.

Soient h_i arrangements (T_k) orthogonaux sur E_i :

$$[x_1^i, x_2^i, \dots, x_k^i; f_j^i(x_1^i, x_2^i, \dots, x_k^i)]$$

$$i \in [1, h], \quad j \in [1, h_i].$$

Soit $n = \min [h_1, h_2, \dots, h_h]$

On définit sur $\mathcal{E} = E_1 \times E_2 \times \dots \times E_h$ les n arrangements (T_k) suivants :

$$[X_1, X_2, \dots, X_k; F_i(X_1, X_2, \dots, X_k)] \quad i \in [1, n],$$

avec les notations :

$$X_1 = (x_1^1, x_1^2, x_1^3, \dots, x_1^h)$$

$$X_2 = (x_2^1, x_2^2, x_2^3, \dots, x_2^h)$$

..

$$X_k = (x_k^1, x_k^2, x_k^3, \dots, x_k^h)$$

et :

$$F_i(X_1, X_2, \dots, X_k) = [f_i^1(x_1^1, x_2^1, \dots, x_k^1), f_i^2(x_1^2, x_2^2, \dots, x_k^2),$$

$$\dots, f_i^h(x_1^h, x_2^h, \dots, x_k^h)]$$

$$i \in [1, n]$$

On a alors le théorème suivant :

Théorème 3.

Les familles ainsi construites définissent sur $\mathcal{E}$ n arrangements (T_k) orthogonaux.

La démonstration est en tous points semblable à celle du théorème 2 : on vérifie à la fois que l'on a bien des arrangements (T_k) et que ces derniers sont orthogonaux.

- L'équivalence entre réseaux $(R)_{k-1}$ permet encore une fois d'énoncer un corollaire :

Corollaire 2.

L'existence de h réseaux $(R)_{k-1}$:

$$\left[E_i, F_i, F_{i,j}, j \in [1, 2, \dots, N_i+k], R_i, q_i, k \right] \\ i \in [1, h]$$

entraîne l'existence d'un réseau $(R)_{k-1}$:

$$\left[E_1 \ E_2 \ \dots \ E_h, F, F_i, \quad i \in [1, 2, \dots, k+\min [h_1 \ h_2 \ \dots \ h_h]] , \right. \\ \left. R, q_1 \ q_2 \ \dots \ q_h , k \right]$$

II. Généralisation de la notion de transversales.

1) - Rappels [réf. [1],[2]].

a) La notion de transversale a été introduite dans l'étude des quasi-groupes mutuellement orthogonaux finis. Elle permettait en particulier de dégager des conditions d'existence. Après avoir rappelé le plus brièvement possible quelques points importants de cette étude, nous généraliserons la définition d'une transversale et serons conduits à établir quelques résultats concernant les réseaux $(R)_{k-1}$.

b) Soit E un ensemble fini, Card [E] = n ; soit ϕ une loi de composition induisant sur E une structure de quasi-groupe (ce qui sera noté $E(\phi)$). On appelle transversale de $E(\phi)$ un ensemble de n couples (x_1^i, x_2^i) , $i = 1, 2, \dots, n$ tels que :

$$\forall (i,j) \in [1,n]^2, i \neq j : x_1^i \neq x_1^j, x_2^i \neq x_2^j \text{ et :} \\ x_1^i \phi x_2^i \neq x_1^j \phi x_2^j.$$

- Toute transversale est donc définie par un sous-ensemble I de $[1, 2, \dots, n]^2$, Card [I] = n, étant entendu que l'on associe à chaque (i,j) de I le couple (x_i, x_j) .

Une transversale peut alors se noter :

$$T = \{ (x_i, x_j, x_i \phi x_j) ; (i,j) \in I \}$$

Théorème 1.

L'existence de n transversales disjointes de $E(\phi)$ est équivalente à l'existence d'un quasi-groupe $E(\psi)$ orthogonal à $E(\phi)$.

En effet, si $E(\psi)$ est un quasi-groupe orthogonal à $E(\phi)$ les sous-ensembles I_k de $(1, 2, \dots, n)^2$:

$$I_k = \{(i, j) ; x_i \psi x_j = x_k\} \quad k \in \{1, 2, \dots, n\}$$

définissent n transversales disjointes :

$$T_k = \{(x_i, x_j, x_i \phi x_j) ; (i, j) \in I_k\} \quad k \in \{1, 2, \dots, n\}$$

et réciproquement.

On peut démontrer alors qu'il existe au plus $(n-1)$ quasi-groupes mutuellement orthogonaux d'ordre n .

- On a d'autre part le théorème :

Théorème 2.

Etant donné un quasi-groupe $E(\phi)$ d'ordre n ($\text{Card } [E] = n$), s'il existe un ensemble transitif de n automorphismes, alors il existe au moins un quasi-groupe orthogonal à $E(\phi)$.

- Un automorphisme θ de $E(\phi)$ est, rappelons-le, une bijection de E sur E , telle que :

$$\theta(x \phi y) = \theta(x) \phi \theta(y) \quad \text{et ceci pour tout couple } (x, y) \text{ de } E^2.$$

Une famille de n automorphismes θ_i , $i \in [1, n]$ est alors transitive, si l'on a la propriété suivante :

$$\forall (x, y) \in E^2, \exists \theta_i \implies y = \theta_i(x).$$

Soit donc une telle famille d'automorphismes.

Pour $a \in E$, à tout $x_k \in E$, associons :

$$T_k = \{(\theta_i(a), \theta_i(x_k), \theta_i(a) \phi \theta_i(x_k)) ; i \in [1, n]\}.$$

On définit ainsi une transversale et il est facile de vérifier que :

$$\forall (k, l) \in [1, n]^2, k \neq l : T_k \cap T_l = \phi.$$

Les n automorphismes transitifs ont donc permis de construire n transversales disjointes et par conséquent un quasi-groupe $E(\psi)$ orthogonal au quasi-groupe $E(\phi)$.

2) - Définitions.

a) Définition d'une transversale.

Soit X un ensemble de q éléments.

Soit un arrangement (T_k) sur X :

$$\begin{aligned} & [x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)] ; \\ & \forall (x_1, x_2, \dots, x_k) \in X^k. \end{aligned}$$

On appelle transversale de $X^k(f)$ un ensemble de q k -tuples (ou points) : $(x_1^i, x_2^i, \dots, x_k^i)$, $i = 1, 2, \dots, q$, tels que :

$$\forall i \neq j, (i, j) \in [1, q]^2, \forall h \in \{1, 2, \dots, k\},$$

l'on ait :

$$x_h^i \neq x_h^j \quad \text{et :}$$

$$f(x_1^i, x_2^i, \dots, x_k^i) \neq f(x_1^j, x_2^j, \dots, x_k^j).$$

- Toute transversale est donc définie par un sous-ensemble I de $[1, 2, \dots, q]^k$, $\text{Card } [I] = q$, étant entendu que l'on associe à chaque élément $(i_1, i_2, \dots, i_k)$ de I , le k -tuple $(x_{i_1}, x_{i_2}, \dots, x_{i_k})$.

Une transversale peut alors être notée :

$$T = \{ (x_{i_1}, x_{i_2}, \dots, x_{i_k} ; f(x_{i_1}, x_{i_2}, \dots, x_{i_k}) ; (i_1, i_2, \dots, i_k) \in I \}$$

b) Définition des sous-transversales d'ordre h ($2 \leq h \leq k$).

Soient les mêmes données, c'est-à-dire X ,

$\text{Card } [X] = q$ et un arrangement (T_k) sur X :

$$(x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)), \forall (x_1, x_2, \dots, x_k) \in X^k.$$

On appelle sous-transversale d'ordre h de $X^k(f)$ occupant la place $(t_1, t_2, \dots, t_h)$, un ensemble de q k -tuples (ou points)

$(x_1^i, x_2^i, \dots, x_k^i)$, $i = 1, 2, \dots, q$, tels que :

$$\forall i \neq j, (i, j) \in [1, q]^2$$

$$\forall h_1 \in \{t_1, t_2, \dots, t_h\}, t_1 \neq t_2 \neq \dots \neq t_h, (t_1, t_2, \dots, t_h) \in [1, k]^h$$

$$\forall h_2 \in \bigcup_{[1, k]} \{t_1, t_2, \dots, t_h\},$$

l'on ait :

$$x_{h_1}^i \neq x_{h_1}^j$$

$$x_{h_2}^i = x_{h_2}^j$$

et :

$$f(x_1^i, x_2^i, \dots, x_k^i) \neq f(x_1^j, x_2^j, \dots, x_k^j).$$

- On voit que $k-h$ variables x_i sont fixées dans chaque k -tuple $(x_1, x_2, \dots, x_k)$ d'une sous-transversale d'ordre h . Il y a donc q^{k-h} valeurs possibles pour ces variables.

- Toute sous-transversale est définie par un sous-ensemble I de $[1, 2, \dots, q]^k$, $\text{Card}[I] = q$, étant entendu que l'on associe à chaque élément $(i_1, i_2, \dots, i_k)$ de I le k -tuple : $(x_{i_1}, x_{i_2}, \dots, x_{i_k})$.

Dans ces conditions, toute sous-transversale peut alors être notée :

$$T = \left\{ (x_{i_1}, x_{i_2}, \dots, x_{i_k}, f(x_{i_1}, x_{i_2}, \dots, x_{i_k})) ; (i_1, i_2, \dots, i_k) \in I \right\}$$

- On dira que l'on a une famille de q^{k-h} sous-transversales d'ordre h occupant la place $(t_1, t_2, \dots, t_h)$ et on la notera $T_{t_1 t_2 \dots t_h}$ si l'on a q^{k-h} sous-transversales d'ordre h dans lesquelles, seules les variables $x_{t_1}, x_{t_2}, \dots, x_{t_h}$ varient, les autres ayant chacune une valeur fixée dans X , aux $k-h$ places restantes notées $i_1, i_2, \dots, i_{k-h}$ de telle façon que chaque $(k-h)$ -tuple $x_{i_1}, x_{i_2}, \dots, x_{i_{k-h}}$ soit obtenu une fois et une seule.

Pour préciser une sous-transversale de la famille

$T_{t_1 t_2 \dots t_h}$ il suffira par conséquent de noter :

$$T_{t_1 t_2 \dots t_h} ; x_{i_1}, x_{i_2}, \dots, x_{i_{k-h}}$$

rappelant ainsi que les valeurs de x_i fixées aux $k-h$ places : $\bigcup_{[1,k]} \{t_1, t_2, \dots, t_h\}$ sont dans l'ordre :

$$x_{i_1}, x_{i_2}, \dots, x_{i_{k-h}}.$$

Exemple.

$T_{1 2 3} ; x_4 x_5 x_6$ désigne la sous-transversale de la famille $T_{1 2 3}$ où x_1, x_2 et x_3 varient tandis que x_4, x_5 et x_6 sont fixées.

Remarque.

Il pourra évidemment arriver que deux sous-transversales d'une même famille ne se différencient que par les valeurs de x_i fixées dans X , mais cela n'est absolument pas une obligation.

- si $h = k$, on retrouve, bien sûr, la définition précédente d'une transversale.
- Deux transversales ou deux sous-transversales seront disjointes si elles n'ont pas de k -tuples $(x_1, x_2, \dots, x_k)$ en commun.

Les k -tuples $(x_1, x_2, \dots, x_k)$ seront par la suite désignés par des points.

Si deux transversales, ou deux sous-transversales ne sont pas disjointes, elles pourront se "couper" en un (ou plusieurs) points.

A remarquer que si : $T_{t_1 t_2 \dots t_h} ; x_{i_1}, x_{i_2}, \dots, x_{i_{k-h}}$ et $T'_{t'_1 t'_2 \dots t'_h} ; x_{i'_1}, x_{i'_2}, \dots, x_{i'_{k-h}}$ peuvent avoir plus d'un point commun, les sous-transversales :

$$T_{t_1 t_2 \dots t_h} ; x_{i_1}, x_{i_2}, \dots, x_{i_{k-h}} \text{ et } T'_{t'_1 t'_2 \dots t'_h} ; x_{i'_1}, x_{i'_2}, \dots, x_{i'_{k-h}}$$

ne peuvent avoir plus d'un point commun.

3) - Construction d'un arrangement (T_k) orthogonal à un arrangement (T_k) donné.

a) Théorème 3.

Soit un ensemble X de q éléments. Soit un arrangement (T_k) sur X :

$$[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)] , \forall (x_1, x_2, \dots, x_k) \in X^k$$

Soit d'autre part un arrangement (T_k) orthogonal à l'arrangement initial :

$$[x_1, x_2, \dots, x_k ; g(x_1, x_2, \dots, x_k)] , \forall (x_1, x_2, \dots, x_k) \in X^k$$

L'existence de ces deux arrangements orthogonaux permet de construire pour tout $t_1 \neq t_2$, $(t_1, t_2) \in [1, k]^2$, q familles de q^{k-2} sous-transversales d'ordre 2, occupant la place (t_1, t_2) , soit $T_{t_1 t_2}^i$, $i \in [1, q]$.

Ces sous-transversales possèdent les propriétés suivantes :

- Deux sous-transversales de deux familles différentes, $T_{t_1 t_2}^i$ et $T_{t_1 t_2}^j$, $i \neq j$, sont disjointes.

$$(\forall t_1 \neq t_2 , (t_1, t_2) \in [1, k]^2).$$

- De même deux sous-transversales quelconques de deux familles différentes $T_{t_1 t_2}^i$ et $T_{t'_1 t'_2}^j$, $i \neq j$, sont disjointes.

$$(\forall t_1 \neq t_2 , (t_1, t_2) \in [1, k]^2 , \forall t'_1 \neq t'_2 , (t'_1, t'_2) \in [1, k]^2).$$

- Soient $T_{t_1 t_2}^i$ et $T_{t'_1 t'_2}^i$ deux familles de sous-transversales.

Les q^{k-2} sous-transversales de chacune de ces deux familles passent par les mêmes points (en nombre q^{k-1}) de X^k .

Ceci est vérifié :

$$\begin{cases} \forall i \in [1, q] \\ \forall (t_1, t_2) \in [1, k]^2 , t_1 \neq t_2 \\ \forall (t'_1, t'_2) \in [1, k]^2 , t'_1 \neq t'_2 \\ (t'_1, t'_2) \neq (t_1, t_2). \end{cases}$$

Remarque.

Les q familles $T_{t_1 t_2}^{\alpha_i}$ constituent une partition de X^k . ($\forall (t_1, t_2)$).

Démonstration.

α) Soit l'égalité :

(1) $g(x_1, x_2, \dots, x_k) = \alpha_i$
 α_i étant fixé dans X , ainsi que $k-2$ x_i , soient $x_{i_1}, x_{i_2}, \dots, x_{i_{k-2}}$. Seules x_{t_1} et x_{t_2} sont variables. Si l'on résout alors l'équation (1) en x_{t_1} et x_{t_2} , on obtient q valeurs pour ce couple : $(x_{t_1}^1, x_{t_2}^1), \dots, (x_{t_1}^q, x_{t_2}^q)$, $1 \in [1, q]$.

D'où q points $(x_1^1, x_2^1, \dots, x_k^1), \dots, (x_1^q, x_2^q, \dots, x_k^q)$, $1 \in [1, q]$

en complétant avec les $k-2$ valeurs $x_{i_1}, x_{i_2}, \dots, x_{i_{k-2}}$ fixées. Ces q points constituent la sous-transversale d'ordre 2 occupant la place (t_1, t_2) :

$$T_{t_1, t_2}^{\alpha_i} ; x_{i_1} x_{i_2} \dots x_{i_{k-2}} = \left\{ (x_1^1, x_2^1, \dots, x_k^1 ; f(x_1^1, x_2^1, \dots, x_k^1) ; 1 \in [1, q] \right\}$$

(Le fait que l'on obtienne une sous-transversale résulte directement du fait que les deux arrangements (T_k) f et g du théorème 3 soient orthogonaux).

β) La construction précédente est, bien sûr, valable pour tout $t_1 \neq t_2$, $(t_1, t_2) \in [1, k]^2$, $\forall \alpha_i \in X$ et quelle que soit la fixation des $k-2$ valeurs $x_{i_1}, x_{i_2}, \dots, x_{i_{k-2}}$. En faisant varier ces paramètres, on obtient q familles de q^{k-2} sous-transversales d'ordre 2 occupant la place (t_1, t_2) : $T_{t_1 t_2}^{\alpha_i}$, $\alpha_i \in X$.

γ) Soient les deux familles :

$$T_{t_1 t_2}^{\alpha_i} \text{ et } T_{t_1 t_2}^{\alpha_j}, \alpha_i \neq \alpha_j.$$

Supposons qu'il existe une sous-transversale T de la première et une sous-transversale T' de la seconde se coupant en un point.

A la sous-transversale T , correspond l'équation : $g(x_1, x_2, \dots, x_k) = \alpha_i$, équation dans laquelle $k-2$ x_i sont fixées : $x_{i1}, x_{i2}, \dots, x_{i_{k-2}}$; x_{t1} et x_{t2} étant seules variables.

De même à la sous-transversale T' , correspond l'équation : $g(x_1, x_2, \dots, x_k) = \alpha_j$, équation dans laquelle $x_{i1}, x_{i2}, \dots, x_{i_{k-2}}$ sont fixées et x_{t1} et x_{t2} sont variables.

(Les variables sont fixées aux mêmes valeurs dans T et T' sinon aucune question ne se poserait quant à leur intersection).

Si T et T' se coupaient en un point $(x_1, x_2, \dots, x_k)$, cela voudrait dire qu'en ce point $g(x_1, x_2, \dots, x_k)$ est égal tantôt à α_i , tantôt à α_j , ce qui est impossible. Deux sous-transversales de deux familles différentes :

$T_{t_1 t_2}^{\alpha_i}$ et $T_{t_1 t_2}^{\alpha_j}$ sont donc bien nécessairement disjointes.

Il s'ensuit que les q familles de q^{k-2} sous-transversales $T_{t_1 t_2}^{\alpha_i}$, $\alpha_i \in X$, constituent une partition de X^k et ceci est valable pour tout (t_1, t_2) , $t_1 \neq t_2$. Pour la même raison que précédemment, il est facile de montrer que, plus généralement, deux sous-transversales de deux familles différentes $T_{t_1 t_2}^{\alpha_i}$ et $T_{t'_1 t'_2}^{\alpha_j}$, $\alpha_i \neq \alpha_j$, $(t_1, t_2) \neq (t'_1, t'_2)$, sont également disjointes.

$\delta)$ Soient enfin deux familles de sous-transversales d'ordre 2 : $T_{t_1 t_2}^{\alpha_i}$ et $T_{t'_1 t'_2}^{\alpha_i}$, $(t_1, t_2) \neq (t'_1, t'_2)$

Les q^{k-1} points des q^{k-2} sous-transversales de chacune de ces deux familles sont solutions de la même équation en $(x_1, x_2, \dots, x_k)$ à savoir :

$$g(x_1, x_2, \dots, x_k) = \alpha_i.$$

On a donc bien :

$$\left\{ T_{t_1 t_2}^{\alpha_i} \right\} = \left\{ T_{t'_1 t'_2}^{\alpha_i} \right\}, \quad \forall (t_1, t_2) \neq (t'_1, t'_2)$$

(équation dans laquelle $\left\{ T_{t_1 t_2}^{\alpha_i} \right\}$ (respectivement $\left\{ T_{t'_1 t'_2}^{\alpha_i} \right\}$) désigne les q^{k-1} points des q^{k-2} sous-transversales de la famille $T_{t_1 t_2}^{\alpha_i}$ (respectivement $T_{t'_1 t'_2}^{\alpha_i}$)).

Finalement, les familles de sous-transversales construites possèdent les propriétés indiquées dans l'énoncé du théorème 3.

c. q. f. d.

b) Théorème 4.

Soit X un ensemble de q éléments. Soit un arrangement (T_k) sur X :

$(x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)) \quad \forall (x_1, \dots, x_k) \in X^k$
 La donnée pour tout $t_1 \neq t_2$ $(t_1, t_2) \in [1, k]^2$ et pour tout $i \in [1, q]$ d'une famille de q^{k-2} sous-transversales d'ordre 2 occupant la place (t_1, t_2) , soit $T_{t_1 t_2}^i$ et possédant les propriétés indiquées dans l'énoncé du théorème 3, entraîne l'existence d'un arrangement (T_k) :
 $(x_1, x_2, \dots, x_k ; g(x_1, x_2, \dots, x_k))$, $\forall (x_1, \dots, x_k) \in X^k$
 orthogonal à l'arrangement (T_k) initial.

Démonstration.

On a vu que les sous-transversales construites précédemment possédaient en particulier les propriétés suivantes :

- deux familles $T_{t_1 t_2}^i$ et $T_{t_1 t_2}^j$, $i \neq j$ étaient disjointes.

- deux familles $T_{t_1 t_2}^i$ et $T_{t'_1 t'_2}^i$ définissaient les mêmes points de X^k (avec les précisions du théorème 3).

On peut, si l'on a des familles de sous-transversales possédant ces propriétés, construire un arrangement (T_k) orthogonal à l'arrangement initial de la façon suivante :

$\alpha)$ $\forall t_1 \neq t_2, (t_1, t_2) \in [1, k]^k$, on associe à $T_{t_1 t_2}^i$ un élément α_i de X de façon biunivoque :

$$i \longleftrightarrow \alpha_i$$

On pose alors pour les q^{k-1} points des sous-transversales de la famille $T_{t_1 t_2}^i$ ($\forall (t_1, t_2)$) :

$$g(x_1, x_2, \dots, x_k) = \alpha_i$$

(Ceci n'est évidemment possible que parce que les familles $T_{t_1 t_2}^i$, i fixé, $t_1 \neq t_2$ quelconques, définissent les mêmes points). Cette construction est répétée pour toutes les valeurs de i et puisque l'on a une partition de X^k , on définit ainsi une application g de X^k dans X .

$$\left(\bigcup_{i \in [1, q]} \left\{ T_{t_1 t_2}^i \right\} \right) = X^k$$

$\beta)$ Il reste à montrer que tout système tiré de I :

$$I \quad \begin{cases} f(x_1, x_2, \dots, x_k) = \alpha & (1) \\ g(x_1, x_2, \dots, x_k) = \alpha_i & (2) \end{cases}$$

à une ou deux équations (respectivement à une ou deux inconnues) a une solution et une seule et l'on aura montré ainsi que l'on a un arrangement (T_k) orthogonal à l'arrangement initial.

Vérifions-le, ce qui suffit dans les deux cas :

- $x_1 = X$, $x_2 = Y$ sont les deux inconnues.

- $x_k = X$ est la seule inconnue dans (2).

- L'équation (2) fixe la sous-transversale :

$$T_{1,2}^{\alpha_i}; x_3 \ x_4 \ \dots \ x_k$$

La 1^o équation fixe un point et un seul de cette sous-transversale.

D'où une solution et une seule (X,Y) pour le système.

Si l'équation (2) a deux solutions en X , soient $(x_1 \ x_2 \ \dots \ X)$ et $(x_1 \ x_2 \ \dots \ X')$ alors :

$$T_{(t_1, k)}^{\alpha_i} x_{i1} \ x_{i2} \ \dots \ x_{ik-2}$$

ne sera plus une sous-transversale, ce qui est contraire à l'hypothèse.

D'où une solution et une seule pour l'équation (2).

4) - Construction de h arrangements (T_k) orthogonaux à un arrangement (T_k) et orthogonaux entre eux sur un ensemble X , $\text{Card } [X] = q$, $1 \leq h \leq k-1$.

a) Théorème 5.

Soit un ensemble X de q éléments. Soit un arrangement (T_k) sur X :

$(x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k))$, $\forall (x_1, \dots, x_k) \in X^k$
permettant de définir des transversales et des sous-transversales.

Soient, d'autre part, h arrangements (T_k) orthogonaux entre eux et orthogonaux à l'arrangement (T_k) initial :

$[x_1, x_2, \dots, x_k ; g_i(x_1, x_2, \dots, x_k)]$, $\forall (x_1, \dots, x_k) \in X^k$
 $i \in [1, h]$, $1 \leq h \leq k-1$.

Il est alors possible de construire :

$$\begin{aligned} & \forall l \in [2, h+1], \\ & \forall (x_{i_1}, x_{i_2}, \dots, x_{i_{k-1}}) \in X^{k-1}, \\ & \forall (t_1, t_2, \dots, t_l) \in [1, k]^l, t_1 \neq t_2 \neq \dots \neq t_l, \\ & \forall (j_1, j_2, \dots, j_{l-1}) \in [1, h]^{l-1}, j_1 \neq j_2 \neq \dots \neq j_{l-1}, \\ & \forall (\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{l-1}}) \in X^{l-1}, \end{aligned}$$

une famille de q^{k-1} sous-transversales d'ordre 1 occupant la place $(t_1, t_2, \dots, t_l)$, soient :

$$\begin{matrix} \alpha_{j_1} & \alpha_{j_2} & \dots & \alpha_{j_{l-1}} \\ T_{t_1} & t_2 & \dots & t_l ; x_{i_1} & x_{i_2} & \dots & x_{i_{k-1}} \end{matrix}$$

Ces familles de sous-transversales possèdent les propriétés suivantes :

α) La disjonction pour les sous-transversales de familles différentes :

$$\begin{matrix} \alpha_{i_1} & \alpha_{i_2} & \dots & \alpha_{i_{l-1}} \\ T_{t_1} & t_2 & \dots & t_l \end{matrix} \quad \text{et} \quad \begin{matrix} \alpha'_{i_1} & \alpha'_{i_2} & \dots & \alpha'_{i_{l-1}} \\ T_{t'_1} & t'_2 & \dots & t'_l \end{matrix}$$

$$\forall l, \forall (t_1, t_2, \dots, t_l), \forall (i_1, i_2, \dots, i_{l-1}),$$

$$\forall (\alpha_{i_1}, \dots, \alpha_{i_{l-1}}) \neq (\alpha'_{i_1}, \dots, \alpha'_{i_{l-1}})$$

et de façon générale, la disjonction pour les sous-transversales de familles différentes :

$$\begin{matrix} \alpha_{i_1} & \alpha_{i_2} & \dots & \alpha_{i_{l-1}} \\ T_{t_1} & t_2 & \dots & t_l \end{matrix} \quad \text{et} \quad \begin{matrix} \alpha'_{i_1} & \alpha'_{i_2} & \dots & \alpha'_{i_{l-1}} \\ T_{t'_1} & t'_2 & \dots & t'_l \end{matrix}$$

$$\forall l, \forall (t_1, t_2, \dots, t_l), \forall (t'_1, t'_2, \dots, t'_l),$$

$$\forall (i_1, i_2, \dots, i_{l-1}), \forall (\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_{l-1}}) \neq$$

$$(\alpha'_{i_1}, \alpha'_{i_2}, \dots, \alpha'_{i_{l-1}}).$$

β) Soient deux familles de sous-transversales différentes :

$$\begin{array}{ccc} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{l-1}} & & \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{l-1}} \\ T_{t_1} t_2 \dots t_l & \text{ET} & T_{t'_1} t'_2 \dots t'_l \end{array}$$

Les q^{k-1} sous-transversales de chacune de ces deux familles passent par les mêmes points de X^k (en nombre q^{k-1+1}).

Ceci est réalisé :

$$\begin{aligned} & \forall 1, \\ & \forall (i_1, i_2, \dots, i_{l-1}) \in [1, h]^{l-1}, i_1 \neq i_2 \neq \dots \neq i_{l-1} \\ & \forall (\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_{l-1}}) \in X^{l-1}, \\ & \forall (t_1, t_2, \dots, t_l) \neq (t'_1, t'_2, \dots, t'_l) \end{aligned}$$

γ) Les q^{k-1+1} points de la famille de sous-transversales

$$\begin{array}{ccc} \alpha_{j_1} \alpha_{j_2} \dots \alpha_{j_{l-1}} \\ T_{t_1} t_2 \dots t_l \end{array}$$

sont inclus dans les q^{k-1+2} points de la famille de sous-transversales

$$\begin{array}{ccc} \alpha'_{j'_1} \alpha'_{j'_2} \dots \alpha'_{j'_{l-2}} \\ T_{t_{i_1}} t_{i_2} \dots t_{i_{l-1}} \end{array}$$

pourvu que :

$$\begin{aligned} & \{t_{i_1}, t_{i_2}, \dots, t_{i_{l-1}}\} \subset \{t_1, t_2, \dots, t_l\}, t_{i_1} \neq t_{i_2} \neq \dots \neq t_{i_{l-1}} \\ & \{\alpha'_{j'_1}, \alpha'_{j'_2}, \dots, \alpha'_{j'_{l-2}}\} \subset \{\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{l-1}}\}, \\ & j'_1 \neq j'_2 \neq \dots \neq j'_{l-2} \end{aligned}$$

Ceci est réalisé :

$$\forall 1, \forall (t_1, t_2, \dots, t_l), \forall (\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{l-1}}).$$

On a de façon précise,

$$\forall t_{i_1} \notin \{t_1, t_2, \dots, t_l\}, \forall j_1 \notin \{j_1, j_2, \dots, j_{l-1}\} :$$

$$\left\{ \begin{matrix} \alpha_{j_1} & \alpha_{j_2} & \dots & \alpha_{j_{l-1}} \\ T_{t_1} & t_2 & \dots & t_1 \end{matrix} \right\} = \bigcup_{\forall \alpha_{j_1} \in X} \left\{ \begin{matrix} \alpha_{j_1} & \alpha_{j_2} & \dots & \alpha_{j_{l-1}} & \alpha_{j_l} \\ T_{t_1} & t_2 & \dots & t_1 & t_{l_1} \end{matrix} \right\}$$

(Notation dans laquelle $\{T\}$ désigne l'ensemble des points de la famille de sous-transversales T).

Remarque.

Les q^{l-1} familles $T_{\begin{matrix} \alpha_{j_1} \alpha_{j_2} \dots \alpha_{j_{l-1}} \\ t_1 t_2 \dots t_1 \end{matrix}}$, constituent un recouvrement en partition de X^k , $\forall l$, $\forall (t_1 t_2 \dots t_1)$.

Démonstration.

La démonstration de ce théorème est en tous points analogue à la démonstration du théorème 4.

Nous indiquerons donc seulement le procédé de construction des sous-transversales.

Soit le système I suivant :

$$I \quad \begin{cases} g_1(x_1, x_2, \dots, x_k) = \alpha_1 & (1) \\ g_2(x_1, x_2, \dots, x_k) = \alpha_2 & (2) \\ \dots & \\ g_h(x_1, x_2, \dots, x_k) = \alpha_h & (h) \end{cases}$$

Considérons les équations (j_1) , (j_2) , ..., (j_{l-1}) extraites du système I. Fixons $\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{l-1}}$ dans X^{l-1} . Faisons varier $x_{t_1}, x_{t_2}, \dots, x_{t_l}$, les autres valeurs des x_i étant fixées : $x_{i_1}, x_{i_2}, \dots, x_{i_{k-1}}$.

Le système ainsi considéré a q solutions (puisque les arrangements (T_k) considérés sont orthogonaux).

Il définit la sous-transversale :

$$\begin{matrix} \alpha_{j_1} & \alpha_{j_2} & \dots & \alpha_{j_{l-1}} \\ T_{t_1} & t_2 & \dots & t_l ; x_{i_1} & x_{i_2} & \dots & x_{i_{k-1}} \end{matrix}$$

(puisque les arrangements (T_k) sont également orthogonaux

à l'arrangement (T_k) initial qui permet de construire des sous-transversales : $[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)]$. Ceci est valable, $\forall (x_{i_1}, x_{i_2}, \dots, x_{i_{k-1}}) \in X^{k-1}$, d'où la famille de sous-transversales :

$$\begin{matrix} \alpha_{j_1} \alpha_{j_2} \dots \alpha_{j_{1-1}} \\ T_{t_1} t_2 \dots t_1 \end{matrix}$$

Cette construction peut être effectuée :

$$\forall 1, \forall (t_1, t_2, \dots, t_1), \forall (j_1, j_2, \dots, j_{1-1}), \forall (\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{1-1}})$$

$$t_1 \neq t_2 \neq \dots \neq t_1, j_1 \neq j_2 \neq \dots \neq j_{1-1}.$$

A remarquer que si $h = k-1$, on obtient en plus des familles de sous-transversales, q^{k-1} transversales ($1 = k$).

b) Théorème 6.

Soit X un ensemble de q éléments. Soit un arrangement (T_k) sur X : $[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)]$ permettant de définir des transversales et des sous-transversales.

La donnée :

$$\left\{ \begin{array}{l} \text{pour tout } 1 \in [2, h+1] \\ \text{pour tout } (t_1, t_2, \dots, t_1) \in [1, k]^{1-1}, t_1 \neq t_2 \neq \dots \neq t_1 \\ \text{pour tout } (j_1, j_2, \dots, j_{1-1}) \in [1, h]^{1-1-1}, j_1 \neq j_2 \neq \dots \neq j_{1-1} \\ \text{pour tout } (\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_{1-1}}) \in X^{1-1-1} \end{array} \right.$$

d'une famille de q^{k-1} sous-transversales d'ordre 1 occupant la place $(t_1, t_2, \dots, t_1)$ soient

$$\begin{matrix} \alpha_{j_1} \alpha_{j_2} \dots \alpha_{j_{1-1}} \\ T_{t_1} t_2 \dots t_1 \end{matrix}$$

possédant les propriétés indiquées au théorème 5 entraîne l'existence de h arrangements (T_k) orthogonaux entre eux et orthogonaux à l'arrangement initial (T_k) sur X . On a : $1 \leq h \leq k-1$.

Démonstration.

La démonstration de ce théorème est analogue à la démonstration du théorème 4.

De la même façon, les familles de sous-transversales $T_{t_1 t_2}^{\alpha_{i_1}}$ permettent de définir l'arrangement (T_k) suivant :

$$[x_1, x_2, \dots, x_k ; \varepsilon_{i_1}(x_1, x_2, \dots, x_k)]$$

avec : $\varepsilon_{i_1}(x_1, x_2, \dots, x_k) = \alpha_{i_1}$.

En faisant varier α_{i_1} dans X et ensuite i_1 dans $[1, h]$, on obtient donc de cette façon h arrangements (T_k) :

$$[x_1, x_2, \dots, x_k ; \varepsilon_i(x_1, x_2, \dots, x_k)] \quad , \quad \forall i \in [1, h] .$$

Il reste à vérifier que ce sont des arrangements orthogonaux entre eux et orthogonaux à l'arrangement initial (T_k) . Cette propriété découle des exigences auxquelles on a soumis les familles de sous-transversales (propriétés énoncées au théorème 5).

Pour alléger l'écriture, nous considérerons un cas particulier mais le raisonnement serait identique dans le cas général.

Soient les familles de sous-transversales suivantes :

$$T_{t_1 t_2}^{\alpha_1} \quad \text{et} \quad T_{t_1 t_2}^{\alpha_2} \quad , \quad t_1 \neq t_2 .$$

On a vu qu'elles permettaient par variation de α_1 dans X et de α_2 dans X de définir deux arrangements (T_k) :

$$(1) : [x_1, x_2, \dots, x_k ; \varepsilon_1(x_1, x_2, \dots, x_k)]$$

$$(2) : [x_1, x_2, \dots, x_k ; \varepsilon_2(x_1, x_2, \dots, x_k)]$$

Le problème qui se pose alors est de savoir si ces deux arrangements (T_k) sont orthogonaux entre eux et orthogonaux à l'arrangement (T_k) initial :

$$[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)] .$$

Nous allons utiliser la propriété générale :

$$\left\{ \begin{matrix} \alpha_{j_1} & \alpha_{j_2} & \dots & \alpha_{j_{l-1}} \\ T_{t_1} & t_2 & \dots & t_l \end{matrix} \right\} = \bigcup_{\alpha_{j_1} \in X} \left\{ \begin{matrix} \alpha_{j_1} & \dots & \alpha_{j_{l-1}} & \alpha_{j_l} \\ T_{t_1} & t_2 & \dots & t_l \end{matrix} \right\}$$

Cette propriété peut s'écrire ici

$$\text{soit : } \left\{ \begin{matrix} \alpha_1 \\ T_{1, 2} \end{matrix} \right\} = \bigcup_{\alpha_2 \in X} \left\{ \begin{matrix} \alpha_1 & \alpha_2 \\ T_{1, 2, 3} \end{matrix} \right\}$$

$$\text{soit : } \left\{ \begin{matrix} \alpha_2 \\ T_{1, 2} \end{matrix} \right\} = \bigcup_{\alpha_1 \in X} \left\{ \begin{matrix} \alpha_1 & \alpha_2 \\ T_{1, 2, 3} \end{matrix} \right\}$$

(On a fixé $t_1 = 1$, $t_2 = 2$, pour simplifier l'écriture).

Considérons alors le système d'équations suivant :

$$\text{I } \begin{cases} g_1(x_1, x_2, \dots, x_k) = \alpha_1 \\ g_2(x_1, x_2, \dots, x_k) = \alpha_2 \end{cases}$$

dans lequel on a fixé $x_3, x_4, \dots, x_k$.

$$\bigcup_{x_3 \in X} \left\{ \begin{matrix} \alpha_1 \\ T_{1, 2 ; x_3 \ x_4 \ \dots \ x_k} \end{matrix} \right\} = \bigcup_{\alpha_2 \in X} \left\{ \begin{matrix} \alpha_1 & \alpha_2 \\ T_{1, 2, 3 ; x_4 \ x_5 \ \dots \ x_k} \end{matrix} \right\}$$

$$\text{et : } \bigcup_{x_3 \in X} \left\{ \begin{matrix} \alpha_2 \\ T_{1, 2 ; x_3, x_4, \dots, x_k} \end{matrix} \right\} = \bigcup_{\alpha_1 \in X} \left\{ \begin{matrix} \alpha_1 & \alpha_2 \\ T_{1, 2, 3 ; x_4 \ x_5 \ \dots \ x_k} \end{matrix} \right\}$$

Fixons x_3 dans la première relation. On fixe donc la sous-transversale :

$$\begin{matrix} \alpha_1 \\ T_{1, 2 ; x_3 \ x_4 \ \dots \ x_k} \end{matrix}$$

Cette dernière est coupée en chacun de ses q points par les sous-transversales $\alpha_1 \ \alpha_2$

$$T_{1, 2, 3 ; x_4 \ x_5 \ \dots \ x_k}$$

En fixant α_2 , on obtient donc un seul point $(x_1, x_2, \dots, x_k)$ d'intersection de

$$\begin{matrix} \alpha_1 \\ T_{1, 2 ; x_3 \ \dots \ x_4} \end{matrix} \text{ avec } \begin{matrix} \alpha_1 & \alpha_2 \\ T_{1, 2, 3 ; x_4 \ \dots \ x_k} \end{matrix}$$

Le même raisonnement peut être répété pour la deuxième relation et l'on obtiendra encore une fois un seul point d'intersection de

$$\alpha_1 \alpha_2 \quad \text{avec} \quad T_{1, 2; x_3 \dots x_k}$$

Ce point d'intersection est nécessairement identique au point précédent puisque x_3 a été fixée à la même valeur dans X.

Le système I ci-dessus a donc une solution et une seule en x_1, x_2 .

Si l'on étudiait maintenant le système :

$$\text{II} \quad \begin{cases} f(x_1, x_2, \dots, x_k) = a \\ g_1(x_1, x_2, \dots, x_k) = \alpha_1 \\ g_2(x_1, x_2, \dots, x_k) = \alpha_2 \end{cases}$$

dans lequel seuls x_1, x_2, x_3 sont variables, il suffirait d'utiliser la sous-transversale :

$$\alpha_1 \alpha_2 \quad T_{1, 2, 3; x_4 \dots x_k}$$

pour être assuré que ce système a une solution et une seule.

c. q. f. d.

5) - Construction de sous-transversales.

a) Soit X un ensemble de q éléments. Soit un arrangement (T_k) sur X :

$$[x_1, x_2, \dots, x_k; f(x_1, x_2, \dots, x_k)] \quad , \quad \forall (x_1, \dots, x_k) \in X^k$$

On dira que les q applications $\alpha_i, i \in [1, q]$ de X dans X sont des automorphismes transitifs si ce sont des bijections possédant les propriétés supplémentaires suivantes :

$$\alpha_i [f(x_1, x_2, \dots, x_k)] = f [\alpha_i(x_1), \alpha_i(x_2), \dots, \alpha_i(x_k)]$$

$$\forall i \in [1, q]$$

$$\text{et : } \forall (a, b) \in X^2 \quad \exists \alpha_i \implies \alpha_i(b) = a.$$

On notera en abrégé le point $[\alpha_i(x_1), \alpha_i(x_2), \dots, \alpha_i(x_k)]$

de la façon suivante : $\alpha_i(x_1, x_2, \dots, x_k)$, $\forall i \in [1, q]$.

b) Soit un arrangement $(T_k) : (x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k))$

Soit un ensemble de q automorphismes transitifs sur X ,

$$\alpha_i, i \in [1, q] .$$

On peut en déduire l'existence de q^{k-1} transversales :

$$\begin{matrix} \alpha_1 & \alpha_2 & \dots & \alpha_{k-1} \\ T_1, & 2, & \dots, & k \end{matrix}$$

Effectivement, soit l'équation : $f(x_1, x_2, \dots, x_k) = a$ avec $a \in X$; $x_1, x_2, \dots, x_k$ étant tous variables dans X .

Cette équation a q^{k-1} solutions $(x_1, x_2, \dots, x_k)_{i_1 i_2 \dots i_{k-1}}$

Soit l'une de ces solutions : $(x_1, x_2, \dots, x_k)_{i_1 i_2 \dots i_{k-1}}$

On peut lui faire correspondre la transversale :

$$\begin{aligned} \alpha_i [(x_1, x_2, \dots, x_k)_{i_1 i_2 \dots i_{k-1}}] &= \\ [\alpha_i(x_1), \alpha_i(x_2), \dots, \alpha_i(x_k)]_{i_1 i_2 \dots i_{k-1}} &, \forall i \in [1, q] . \end{aligned}$$

D'où par variation de $(i_1 i_2 \dots i_{k-1})$ l'existence des q^{k-1} transversales annoncées.

Il est à remarquer que ce procédé ne permet pas de construire des sous-transversales et que l'on ne peut donc en déduire l'existence d'arrangements (T_k) orthogonaux.

III. Construction d'arrangements (T_k) idempotents et d'arrangements (T_k) isotopes (réf. [1], [3], [4], [5], [6], [9], [10])

A) Introduction.

Les deux notions d'isotopie et d'idempotence ont été étudiées dans le cas des quasi-groupes. Cela était

nécessaire, l'idempotence étant parfois requise pour les familles de quasi-groupes mutuellement orthogonaux à construire et l'isotopie permettant des constructions faciles de quasi-groupes.

Nous généraliserons dans ce paragraphe successivement ces deux notions au cas des arrangements (T_k) et étudierons le cas des arrangements (T_k) orthogonaux.

2) Définitions.

a) Définition d'un arrangement (T_k) idempotent.

Soit X un ensemble de q éléments. Soit un arrangement (T_k) sur X :

$$[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)]$$

On dira que cet arrangement (T_k) est idempotent si et seulement si :

$$\forall x \in X : f(x, x, \dots, x) = x$$

b) Définition d'arrangements (T_k) isotopes.

Soit X un ensemble de q éléments. Soit un arrangement (T_k) sur X :

$$[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)]$$

L'arrangement $(T_k)^1$ sur X :

$$[x_1, x_2, \dots, x_k ; g(x_1, x_2, \dots, x_k)]$$

sera isotope de l'arrangement (T_k) initial si et seulement s'il existe des bijections $f_1, f_2, \dots, f_{k+1}$ de X sur X telles que :

$$g(x_1, x_2, \dots, x_k) = a \quad \text{soit équivalent à :}$$

$$f[f_1(x_1), f_2(x_2), \dots, f_k(x_k)] = f_{k+1}(a)$$

$$\left\{ \begin{array}{l} \forall (x_1, x_2, \dots, x_k) \in X^k \\ \forall a \in X \end{array} \right.$$

L'arrangement $(T_k)^1$ sera dit isotope - Do si la

bijection f_{k+1} se réduit à l'application identique I.

3) Construction d'arrangements (T_k) idempotents.

a) Rappels.

α) Nous employons ici les notations de H.B. Mann (réf. [3] et [4]).

Soient A et B deux carrés latins. Pour qu'ils soient orthogonaux, il faut et il suffit qu'il existe un carré latin C tel que : $AC = B$.

Si le carré latin A est orthogonal au carré latin B, alors PAQ est orthogonal à PBR pour toutes permutations P, Q, R.

Ces deux résultats peuvent s'écrire de la façon suivante dans le langage de la théorie des quasi-groupes :

- Soient deux quasi-groupes $E(\theta)$ et $E(\phi)$. Pour qu'ils soient orthogonaux, il faut et il suffit qu'il existe un quasi-groupe $E(\psi)$ tel que :

$$x \psi [x \phi y] = x \theta y \quad \forall (x, y) \in E^2$$

- Soient deux quasi-groupes orthogonaux $E(\theta)$ et $E(\phi)$. Les quasi-groupes suivants sont orthogonaux pour toutes bijections p, q, r.

$$x \theta_1 y = q [x \theta p(y)]$$

$$x \phi_1 y = r [x \phi p(y)]$$

β) Soit un quasi-groupe $E(\phi)$; quel que soit $e \in E$, il existe une isotopie transformant $E(\phi)$ en une boucle admettant e comme élément unité. ([1])

Il suffit de considérer les bijections :

$$p : x \longrightarrow e \phi x$$

$$q : x \longrightarrow x \phi p^{-1}(e)$$

pour construire la boucle $E(\psi)$:

$$x \psi y = q^{-1}(x) \psi p^{-1}(y).$$

7) Soit un quasi-groupe $E(\phi)$; il existe une isotopie transformant $E(\phi)$ en un quasi-groupe $E(\psi)$ telle que :

$$\exists e \in E, \quad \forall x \in E, \quad e \psi x = x.$$

En effet, soit e un élément quelconque de E . $\forall x \in E$, $e \phi x$ décrit E : $p(x) = e \phi x$ est une bijection de E sur E et on a :

$$p^{-1}(e \phi x) = x$$

D'où la structure $E(\psi)$ cherchée :

$$x \psi y = p^{-1}(x \phi y).$$

- Etant donné m quasi-groupes mutuellement orthogonaux, à $m-1$ d'entre eux, on peut faire correspondre $(m-1)$ quasi-groupes mutuellement orthogonaux idempotents (réf. [1]). En effet, soient $E(\theta_i)$, $i \in [1, m]$ les m quasi-groupes mutuellement orthogonaux. Par isotopie, on peut les transformer en m quasi-groupes mutuellement orthogonaux $E(\phi_i)$, $i \in [1, m]$, tels que : $\exists a \quad \forall i \in [1, m] \quad \forall y \in E \implies a \phi_i y = y$.

On associe alors à tout (x, y) de E^2 , z tel que : $x = z \phi_1 y$, et on considère les opérations ψ_j :

$$\forall (x, y) \in E^2, \quad x \psi_j y = z \phi_j y, \quad \forall j \in [2, m]$$

$E(\psi_j)$, $j \in [2, m]$ forment une classe de $m-1$ quasi-groupes mutuellement orthogonaux idempotents.

6) Application aux arrangements (T_k) .

$\alpha)$ Généralisation des théorèmes de H. B. Mann
([3] et [4]).

Théorème 1.

Soit X un ensemble de q éléments. Soient h arrangements (T_k) sur X :

$$[(x_1, x_2, \dots, x_k; f_i(x_1, x_2, \dots, x_k))] \quad i \in [1, h]$$

Les conditions suivantes sont équivalentes :

(a) - Les h arrangements (T_k) sont orthogonaux :

$$\begin{cases} f_1(x_1, x_2, \dots, x_k) = a^1 \\ f_2(x_1, x_2, \dots, x_k) = a^2 \\ \dots \\ f_h(x_1, x_2, \dots, x_k) = a^h \end{cases}$$

(b) - $\forall t \in [2, \min [h, k]]$, $\forall (a^{i_1}, a^{i_2}, \dots, a^{i_t})$ extrait de $(a^1, a^2, \dots, a^h)$, $i_1 \neq i_2 \neq \dots \neq i_t$,

$\forall (x_{j_1}, x_{j_2}, \dots, x_{j_t})$ extrait de $(x_1, x_2, \dots, x_k)$, $j_1 \neq j_2 \neq \dots \neq j_t$, il existe $t-1$ arrangements (T_t) :

$$[y_1 y_2 \dots y_t ; g_j(y_1 y_2 \dots y_t)]$$

$$\begin{cases} y_i \in X \\ i \in [1, t] \\ j \in [1, t-1] \end{cases}$$

tels que : $\forall (x_1 x_2 \dots x_k) \in X^k$, l'on ait :

$$g_j [x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, f_{i_1}(x_1, x_2, \dots, x_k)] = f_{i_j}(x_1, x_2, \dots, x_k) \quad \forall j \in [2, t]$$

et tels que les arrangements $(T)_{t-1}$ suivants soient orthogonaux :

$$[y_1, y_2, \dots, y_{t-1}, g_j(y_1, y_2, \dots, y_{t-1}, a)] , \begin{cases} \forall j \in [1, t-1] \\ \forall a \in X \\ a \text{ fixé.} \end{cases}$$

Démonstration.

Soit le système I suivant :

$$I \begin{cases} f_1(x_1, x_2, \dots, x_k) = a^1 & (1) \\ f_2(x_1, x_2, \dots, x_k) = a^2 & (2) \\ \dots & \vdots \\ f_h(x_1, x_2, \dots, x_k) = a^h & (h) \end{cases}$$

Démontrons que (a) $\implies$ (b).

Tout système extrait de I à t équations $i_1 \ i_2 \dots i_t$ et à t inconnues $x_{j_1}, x_{j_2}, \dots, x_{j_t}$ doit avoir une solution et une seule, $\forall t \in [2, \min [h, k]]$, par hypothèse :

$$\text{II} \quad \begin{cases} a_{i_1} = f_{i_1}(x_1, x_2, \dots, x_k) & (i_1) \\ a_{i_2} = f_{i_2}(x_1, x_2, \dots, x_k) & (i_2) \\ \dots \\ a_{i_t} = f_{i_t}(x_1, x_2, \dots, x_k) & (i_t) \end{cases}$$

Donc si $a_{i_1} \ a_{i_2} \dots a_{i_t}$ sont fixés, on en déduit l'existence d'une valeur et d'une seule pour chacune des variables $x_{j_1}, x_{j_2}, \dots, x_{j_t}$. Si l'on utilise l'équation (i_1) , on peut exprimer x_{j_t} en fonction de $x_{j_1} \ x_{j_2} \dots x_{j_{t-1}}$ et a_{i_1} ; on obtient ainsi :

$$x_{j_t} = h(x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, a_{i_1})$$

et le système II s'écrit :

$$\begin{cases} a_{i_2} = f_{i_2} [x_1, x_2, \dots, h(x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, a_{i_1}), \dots, x_k] \\ \dots \\ a_{i_t} = f_{i_t} [x_1, x_2, \dots, h(x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, a_{i_1}), \dots, x_k] \end{cases}$$

avec : $x_{j_t} = h(x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, a_{i_1})$

c'est-à-dire :

$$\begin{cases} a_{i_2} = g_{i_2} (x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, a_{i_1}) \\ \dots \\ a_{i_t} = g_{i_t} (x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, a_{i_1}) \\ a_{i_1} = f_{i_1}(x_1, x_2, \dots, x_k) \end{cases}$$

Dès lors $a \implies b$ pourvu que :

$$- [y_1 \ y_2 \dots y_t ; g_{i_j}(y_1, y_2, \dots, y_t)] \quad \forall j \in [2, t]$$

soit un arrangement $(T)_t$ et si :

- $(y_1, y_2, \dots, y_{t-1}; g_{ij}(y_1, y_2, \dots, y_{t-1}, a))$ sont des arrangements $(T)_{t-1}$ orthogonaux pour tout a fixé dans X ($j \in [2, t]$).

Ces deux propriétés sont faciles à vérifier. Vérifions tout d'abord que l'on a des arrangements $(T)_t$. Autrement dit, vérifions par exemple que l'équation :

$$g_{i2}(X, x_{j2}, \dots, a_{i1}) = a_{i2}$$

a une solution et une seule en X ($x_{j2}, x_{j3}, \dots, x_{jt-1}, a_{i1}, a_{i2}$ étant fixes).

Si l'on suppose par l'absurde l'existence de 2 solutions x_{j1} et $x_{j'1}$, le système suivant :

$$\begin{cases} f_{i1}(x_1 \ x_2 \ \dots \ x_k) = a_{i1} \\ f_{i2}(x_1 \ x_2 \ \dots \ x_k) = a_{i2} \end{cases}$$

aurait plusieurs solutions en x_{j1} et x_{jt} , ce qui est contraire à l'hypothèse.

Vérifions enfin que les arrangements $(T)_{t-1}$ sont orthogonaux. Soit pour alléger l'écriture le système :

$$\begin{cases} g_{i2}(X, Y, x_{j3}, \dots, x_{jt-1}, a) = a_{i2} \\ g_{i3}(X, Y, x_{j3}, \dots, x_{jt-1}, a) = a_{i3} \end{cases}$$

de deux équations à 2 inconnues X et Y . S'il avait plusieurs solutions, le système :

$$\begin{cases} f_{i1}(x_1 \ \dots \ x_k) = a \\ f_{i2}(x_1 \ \dots \ x_k) = a_{i2} \\ f_{i3}(x_1 \ \dots \ x_k) = a_{i3} \end{cases}$$

de 3 équations à 3 inconnues x_{j1}, x_{j2} et x_{jt} aurait plusieurs solutions, ce qui est également contraire à l'hypothèse. Finalement $a) \implies b)$ et la réciproque $b) \implies a)$ suit facilement.

(l'énoncé de ce théorème est à rapprocher de la démarche de résolution d'un système de n équations à n inconnues par élimination successive des variables).

Théorème 2.

Soient h arrangements (T_k) orthogonaux sur X :

$(x_1, x_2, \dots, x_k ; a^i)$ avec :

$$a^i = f_i(x_1, x_2, \dots, x_k) \quad , i \in [1, h] .$$

Les h arrangements (T_k) sur X suivants :

$(x_1, x_2, \dots, x_k ; b^i)$ avec :

$$b^i = p_i \left[f_i(q_1(x_1), q_2(x_2), \dots, q_k(x_k)) \right] ,$$

$\forall i \in [1, h]$ sont orthogonaux, quelles que soient les bijections $p_1 p_2 \dots p_h$, $q_1 q_2 \dots q_k$ de X sur X .

La démonstration utilisant la définition des arrangements orthogonaux (T_k) est immédiate.

$\beta)$ Construction d'arrangements (T_k) idempotents.

Théorème 3.

Soit X un ensemble fini de q éléments. Soient h arrangements (T_k) orthogonaux sur X :

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)] \quad , i \in [1, h]$$

A $h-k+1$ d'entre eux, on peut faire correspondre $(h-k+1)$ arrangements (T_k) orthogonaux et idempotents.

Démonstration.

Cette construction est une généralisation de celle effectuée par Guérin (réf. [1]) à propos des quasi-groupes mutuellement orthogonaux et idempotents.

A $(x_1, x_2, \dots, x_k) \in X^k$, on associe $(z_1, z_2, \dots, z_{k-1}) \in X^{k-1}$ de la façon suivante :

$$I \quad \begin{cases} x_1 = f_1(z_1, z_2, \dots, z_{k-1}, x_k) \\ x_2 = f_2(z_1, z_2, \dots, z_{k-1}, x_k) \\ \dots \\ x_{k-1} = f_{k-1}(z_1, z_2, \dots, z_{k-1}, x_k) \end{cases}$$

$x_1, x_2, \dots, x_k$ fixes, fixent donc une valeur et une seule pour $z_1, z_2, \dots, z_{k-1}$, puisque les arrangements (T_k) considérés sont orthogonaux par hypothèse.

On pose alors pour tout $i \in [k; h]$

$$\underline{F_i(x_1, x_2, \dots, x_k) = f_i(z_1, z_2, \dots, z_{k-1}, x_k)}$$

$z_1, z_2, \dots, z_{k-1}$ étant déterminés par le système I.

Nous allons vérifier que nous avons ainsi construit $h-k+1$ arrangements (T_k) orthogonaux :

$$[x_1, x_2, \dots, x_k; F_i(x_1, x_2, \dots, x_k)] \quad \forall i \in [k, h]$$

En effet, vérifions tout d'abord que l'on a bien obtenu des arrangements (T_k) . Considérons pour cela l'équation :

$$F_j(x_1, x_2, \dots, x_k) = \alpha$$

où x_i seul varie.

Du système I dont on a retiré la $i^{\text{ème}}$ ligne et auquel on ajoute $F_j(x_1, x_2, \dots, x_k) = \alpha$, soit :

$$\begin{cases} x_1 = f_1(z_1, z_2, \dots, z_{k-1}, x_k) \\ \dots \\ x_{i-1} = f_{i-1}(z_1, z_2, \dots, z_{k-1}, x_k) \\ x_{i+1} = f_{i+1}(z_1, z_2, \dots, z_{k-1}, x_k) \\ \dots \\ x_{k-1} = f_{k-1}(z_1, z_2, \dots, z_{k-1}, x_k) \\ f_j(z_1, z_2, \dots, z_{k-1}, x_k) = \alpha \end{cases}$$

On tire une solution et une seule $(z_1^*, z_2^*, \dots, z_{k-1}^*)$ pour les variables $z_1, z_2, \dots, z_{k-1}$.

L'équation :

$$F_j(x_1, x_2, \dots, x_k) = \alpha$$

a donc une solution et une seule en x_i , soit :

$$x_i = f_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x_k)$$

(Si x_k était variable, le résultat serait acquis immédiatement puisque les arrangements sont orthogonaux).

Nous avons donc bien construit $h-k+1$ arrangements (T_k) et nous allons maintenant vérifier qu'ils sont orthogonaux.

Soit donc le système de t équations suivant :

$$\text{II} \quad \begin{cases} F_{i1}(x_1, x_2, \dots, x_k) = \alpha_1 \\ F_{i2}(x_1, x_2, \dots, x_k) = \alpha_2 \\ \dots \\ F_{it}(x_1, x_2, \dots, x_k) = \alpha_t \end{cases}$$

dans lequel $x\alpha_1, x\alpha_2, \dots, x\alpha_t$ sont les seules variables. Du système I dont on a retiré les lignes $\alpha_1, \alpha_2, \dots, \alpha_t$ et auquel on ajoute le système II, on tire une solution et une seule $(z_1^*, z_2^*, \dots, z_{k-1}^*)$ pour les variables $(z_1 \dots z_{k-1})$ et le système II a donc une solution et une seule en $x\alpha_1, x\alpha_2, \dots, x\alpha_t$.

Il ne reste plus qu'à transformer les arrangements obtenus en arrangements idempotents pour que le résultat soit acquis.

Nous allons tout d'abord remplacer les $k-1$ premiers arrangements (T_k)

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)] \quad , \quad \forall i \in [1, k-1]$$

par des arrangements (T_k) isotopes :

$$[x_1, x_2, \dots, x_k ; f'_i(x_1, x_2, \dots, x_k)] \quad , \forall i \in [1, k-1]$$

de façon à ce que :

$$\underline{f'_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x) = x \quad \forall x \in X \quad , \quad \forall i \in [1, k-1]}$$

$z_1^*, z_2^*, \dots, z_{k-1}^*$ étant fixés en valeur dans X .

Pour cela fixons arbitrairement $z_1, z_2, \dots, z_{k-1}$ aux valeurs $z_1^*, z_2^*, \dots, z_{k-1}^*$ et considérons la bijection θ_i de X sur X , $\forall i \in [1, k-1]$ telle que :

$$x \in X \xrightarrow{\theta_i} f_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x) \in X.$$

Soient alors $\forall i \in [1, k-1]$, les arrangements (T_k) isotopes définis par :

$$[x_1, x_2, \dots, x_k ; f'_i(x_1, x_2, \dots, x_k)]$$

et :

$$\underline{f'_i(x_1, x_2, \dots, x_k) = \theta_i^{-1} [f_i(x_1, x_2, \dots, x_k)]}$$

Les $k-1$ arrangements (T_k) ainsi construits sont encore orthogonaux entre eux et orthogonaux aux arrangements (T_k) restants ($i \in [k, h]$).

Ils jouissent d'autre part de la propriété cherchée, à savoir :

$$\text{si } \begin{cases} x_1 = z_1^* \\ x_2 = z_2^* \\ \vdots \\ x_{k-1} = z_{k-1}^* \\ x_k \text{ quelconque} \end{cases}$$

on a :

$$\begin{aligned} f'_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x_k) &= \theta_i^{-1} [f_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x_k)] \\ &= x_k \end{aligned}$$

Nous avons donc réussi à remplacer les $k-1$ premiers arrangements (T_k) orthogonaux par des arrangements (T_k) orthogonaux ayant la propriété indiquée.

Pour simplifier l'écriture, nous supposons simplement dans la suite que les arrangements (T_k) primitifs jouissaient déjà de cette propriété (ce qui revient à confondre l'écriture f'_i avec f_i et ceci $\forall i \in [1, k-1]$). Dans ces conditions, il est bien évident que l'application η_i de X dans X suivante :

$$x \in X \xrightarrow{\eta_i} f_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x) \in X$$

est une bijection de X sur X , $\forall i \in [k, h]$ et rappelons que l'on a la propriété :

$$\begin{cases} x = f_1(z_1^*, z_2^*, \dots, z_{k-1}^*, x) \\ x = f_2(z_1^*, z_2^*, \dots, z_{k-1}^*, x) \\ \vdots \\ x = f_{k-1}(z_1^*, z_2^*, \dots, z_{k-1}^*, x) \\ \forall x \in X \end{cases}$$

Remplaçons alors les $h-k+1$ arrangements (T_k) :

$$[x_1, x_2, \dots, x_k ; F_i(x_1, x_2, \dots, x_k)] \quad \forall i \in [k, h]$$

par les arrangements (T_k) isotopes suivants :

$$[x_1, x_2, \dots, x_k ; G_i(x_1, x_2, \dots, x_k)] \quad \forall i \in [k, h]$$

définis par :

$$G_i(x_1, x_2, \dots, x_k) = \eta_i^{-1}[F_i(x_1, x_2, \dots, x_k)]$$

$$\forall i \in [k, h].$$

Les $h-k+1$ arrangements (T_k) ainsi obtenus sont encore orthogonaux et ils sont en outre idempotents :

$$\begin{aligned} G_i(x, x, \dots, x) &= \prod_i^{-1} [F_i(x, x, \dots, x)] \\ &= \prod_i^{-1} [f_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x)] \\ &= x \end{aligned}$$

c. q. f. d.

Remarque.

Du fait que : $f_i(z_1^*, z_2^*, \dots, z_{k-1}^*, x) = x$,
 $\forall x \in X$, $\forall i \in [1, k-1]$

la solution du système :

$$\begin{cases} x = f_1(z_1, z_2, \dots, z_{k-1}, x) \\ x = f_2(z_1, z_2, \dots, z_{k-1}, x) \\ \vdots \\ x = f_{k-1}(z_1, z_2, \dots, z_{k-1}, x) \end{cases}$$

est nécessairement : $z_i = z_i^*$, $\forall i \in [1, k-1]$

quelle que soit la valeur de x fixée dans X .

Nous allons examiner maintenant le cas particulier où il existe un ensemble d'automorphismes transitifs (ce que l'on désigne dans l'étude des quasi-groupes par quasi-groupes homogènes) et voir que dans ce cas, on construit h arrangements (T_k) orthogonaux et idempotents, à partir de h arrangements (T_k) orthogonaux.

Théorème 4.

Soient h arrangements (T_k) orthogonaux sur un ensemble X de q éléments :

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)] \quad , \quad i \in [1, h] .$$

Supposons que le groupe des automorphismes sur X soit transitif, on peut alors construire sur X h arrangements orthogonaux (T_k) idempotents :

$$[x_1, x_2, \dots, x_k ; \varepsilon_i(x_1, x_2, \dots, x_k)] \quad , \quad i \in [1, h]$$

$$\varepsilon_i(x, x, \dots, x) = x \quad \forall x \in X \quad , \forall i \in [1, h] \quad .$$

Démonstration.

Soient $\alpha_i \quad i \in [1, h]$ les éléments du groupe des automorphismes.

(Rappelons que les α_i sont des bijections de X sur X telles que :

$$(1) \quad \forall (a, b) \in X^2 \quad \exists \alpha_i \implies \alpha_i(b) = a.$$

$$(2) \quad \forall i, \forall j, \alpha_i [f_j(x_1, x_2, \dots, x_k)] =$$

$$f_j[\alpha_i(x_1), \alpha_i(x_2), \dots, \alpha_i(x_k)] \quad .$$

Soit $\forall i \in [1, h] \quad \theta_i$ l'application de X dans X définie par :

$$x \xrightarrow{\theta_i} f_i(x, x, \dots, x)$$

Nous allons vérifier que $\forall i \in [1, h] \quad \theta_i$ est une bijection de X sur X .

Il suffit de vérifier pour cela que θ_i est une surjection de X sur X .

Effectivement, soient a et c deux éléments de X .

Soit $b = f_i(a, a, \dots, a)$.

On sait qu'il existe un automorphisme α_j tel que :

$$\alpha_j(b) = c$$

On a alors :

$$c = \alpha_j(b) = \alpha_j [f_i(a, a, \dots, a)]$$

$$= f_i [\alpha_j(a), \alpha_j(a), \dots, \alpha_j(a)]$$

$$= \theta_i [\alpha_j(a)]$$

En résumé donc : $c = \theta_i [\alpha_j(a)]$.

On voit donc que pour tout $c \in X$ il existe un élément de X , soit $\alpha_j(a)$ tel que :

$$c = \theta_i [\alpha_j(a)] \quad .$$

On a donc bien démontré que θ_i est une surjection $\forall i \in [1, h]$ et par conséquent une bijection de X .

Soient alors les arrangements (T_k) suivants :

$$[x_1, x_2, \dots, x_k ; g_i(x_1, x_2, \dots, x_k)] \quad \forall i \in [1, h]$$

définis par :

$$g_i(x_1, x_2, \dots, x_k) = \theta_i^{-1} [f_i(x_1, x_2, \dots, x_k)]$$

Ce sont des arrangements orthogonaux puisque les arrangements f_i initiaux étaient orthogonaux.

D'autre part :

$$g_i(x, x, \dots, x) = \theta_i^{-1} [f_i(x, x, \dots, x)] = x \quad \forall i \in [1, h] .$$

Ce sont donc des arrangements idempotents.

c. q. f. d.

4) Construction d'arrangements (T_k) isotopes.

a) Nous allons tout d'abord chercher les conditions pour que, un arrangement (T_k) étant donné, un arrangement (T_k^1) isotope - Do de l'arrangement (T_k) initial, soit orthogonal à l'arrangement (T_k) . Par définition, un arrangement (T_k^1) isotope-Do de l'arrangement (T_k) peut s'écrire :

$$[x_1, x_2, \dots, x_k ; F [f_1(x_1), f_2(x_2), \dots, f_k(x_k)]] ,$$

si l'arrangement initial (T_k) s'écrit :

$$[x_1, x_2, \dots, x_k ; F(x_1, x_2, \dots, x_k)]$$

et si $f_1, f_2, \dots, f_k$ sont des bijections de X sur X .

(T_k) et (T_k^1) seront alors des arrangements orthogonaux si et seulement si le système I :

$$I \quad \begin{cases} F(x_1, x_2, \dots, x_k) = a \\ F[f_1(x_1), f_2(x_2), \dots, f_k(x_k)] = b \end{cases}$$

de deux équations à deux inconnues x_{t_1} et x_{t_2} a une solution et une seule et ceci

$$\forall (a, b) \in X^2, \forall (t_1, t_2) \in [1, k]^2, t_1 \neq t_2, \forall x_i \in X \\ \forall i \neq \{t_1, t_2\}.$$

Supposons tout d'abord que X soit muni d'une structure de groupe abélien notée additivement et que :

$$F(x_1, x_2, \dots, x_k) = x_1 + x_2 + \dots + x_k$$

Supposons d'autre part que les bijections f_i , $\forall i \in [1, k]$ soient des automorphismes de X sur X muni de cette structure. Le système I s'écrit dans ces conditions :

$$II \quad \begin{cases} x_1 + x_2 + \dots + x_k = a \\ f_1(x_1) + f_2(x_2) + \dots + f_k(x_k) = b. \end{cases}$$

Prenons pour alléger l'écriture $t_1 = 1$, $t_2 = 2$.

Si l'on suppose, par l'absurde, que le système II admet 2 solutions (x_1, x_2) et (x'_1, x'_2) , l'on a :

$$\begin{cases} x_1 + x_2 = x'_1 + x'_2 = \alpha & , \quad \alpha \text{ fixée dans } X \\ f_1(x_1) + f_2(x_2) = f_1(x'_1) + f_2(x'_2) = \beta & , \quad \beta \text{ fixée dans } X \end{cases}$$

c'est-à-dire :

$$f_1^{-1} f_2(x_2) - x_2 = f_1^{-1} f_2(x'_2) - x'_2 = \gamma, \quad \gamma \text{ fixée dans } X$$

d'où le théorème suivant :

Théorème 5. ([1] , [5] et [6])

Les arrangements (T_k) et (T_k^1) sont orthogonaux si et seulement si :

$$\forall i \neq j : f_i^{-1} f_j(x) - x = u$$

a une solution et une seule en x , $\forall u \in X$.

Remarque.

Puisque les bijections f_i sont des automorphismes, il est bien certain que si $f_i^{-1} f_j(x) - x = u$ a une solution et une seule en x , $\forall u \in X$, il en est de même pour : $f_j^{-1} f_i(x) - x = u$, $\forall u \in X$.

Définition.

Une bijection θ d'un groupe X sur lui-même est un orthomorphisme si et seulement si :

$$\forall (x, y) \in X^2, \quad \theta(x) - x = \theta(y) - y \implies x = y.$$

Un automorphisme d'un groupe X est alors un orthomorphisme si et seulement si l'élément neutre 0 du groupe X est le seul point fixe de l'automorphisme.

Dans le théorème précédent, la condition requise est donc que $f_i^{-1} f_j$ soit un orthomorphisme ou bien que $f_i^{-1} f_j$ soit un automorphisme admettant 0 comme seul point fixe.

b) On peut se poser le même problème que précédemment pour deux isotopes-Do, (T_k^1) et (T_k^3) de l'arrangement (T_k) initial.

Autrement dit, chercher les conditions requises pour que le système I :

$$I \quad \begin{cases} f_1(x_1) + f_2(x_2) + \dots + f_k(x_k) = a \\ g_1(x_1) + g_2(x_2) + \dots + g_k(x_k) = b \end{cases}$$

de deux équations à deux inconnues x_{t_1} et x_{t_2} ait une solution et une seule et ceci :

$$\forall (a, b) \in X^2, \quad \forall (t_1, t_2) \in [1, k]^2, \quad t_1 \neq t_2, \quad \forall x_i \in X, \\ \forall i \neq (t_1, t_2)$$

$f_1, f_2, \dots, f_k, g_1, g_2, \dots, g_k$ étant des automorphismes du groupe X sur lui-même.

Prenons encore une fois pour simplifier l'écriture :

$$t_1 = 1, \quad t_2 = 2.$$

Le système I s'écrit :

$$\text{II} \quad \begin{cases} f_1(x_1) + f_2(x_2) = \alpha \\ g_1(x_1) + g_2(x_2) = \beta \end{cases} \quad \begin{array}{l} \alpha \text{ fixée dans } X \\ \beta \text{ fixée dans } X \end{array}$$

c'est-à-dire :

$$x_1 + f_1^{-1} f_2(x_2) = \alpha$$

$$x_1 + g_1^{-1} g_2(x_2) = \beta$$

Le système I aura donc finalement une solution et une seule si et seulement si :

$\forall i \neq j, \quad g_j^{-1} g_i f_i^{-1} f_j$ est un orthomorphisme d'où le théorème :

Théorème 6 ([1] et [6])

Soit un groupe $X(+)$. Soient $f_i, i \in [1, k], g_i, i \in [1, k], 2k$ automorphismes sur X .

Le système :

$$\begin{cases} f_1(x_1) + f_2(x_2) + \dots + f_k(x_k) = a \\ g_1(x_1) + g_2(x_2) + \dots + g_k(x_k) = b \end{cases}$$

de deux équations à deux inconnues x_{t_1} et x_{t_2} a une solution et une seule, $\forall (a, b) \in X^2, \forall (t_1, t_2) \in [1, k]^2,$

$t_1 \neq t_2, \forall x_i \in X, \forall i \neq (t_1, t_2)$ si et seulement si :

$\forall i \neq j, \quad g_j^{-1} g_i f_i^{-1} f_j$ est un orthomorphisme.

Remarques.

$\propto$) Il revient au même d'exiger dans l'énoncé du théorème précédent que $g_j^{-1} g_i f_i^{-1} f_j$ soit un automorphisme admettant 0 l'élément neutre de X comme seul point fixe.

De façon analogue, si l'on considère l'endomorphisme

$f_i^{-1}f_j - g_i^{-1}g_j$ qui associe à x la quantité :

$$(f_i^{-1}f_j - g_i^{-1}g_j)(x) = f_i^{-1}f_j(x) - g_i^{-1}g_j(x)$$

Il revient au même d'exiger dans l'énoncé du théorème précédent que l'endomorphisme $f_i^{-1}f_j - g_i^{-1}g_j$ soit un automorphisme.

β) Il est facile de justifier que si $g_j^{-1}g_i f_i^{-1}f_j$ est un orthomorphisme, de même les automorphismes :

$g_i^{-1}g_j f_j^{-1}f_i$, $f_i^{-1}f_j g_j^{-1}g_i$, $f_j^{-1}f_i g_i^{-1}g_j$ sont des orthomorphismes et réciproquement.

En effet, soit par exemple $g_i^{-1}g_j f_j^{-1}f_i$.

L'équation : $g_j^{-1}g_i(x) - f_j^{-1}f_i(x) = u$ doit avoir une solution et une seule.

Cette dernière s'écrit :

$$g_i(x) - g_j f_j^{-1}f_i(x) = u$$

Soit en posant $y = f_i(x)$:

$$g_i f_i^{-1}(y) - g_j f_j^{-1}(y) = u$$

Soit en posant $f_j^{-1}(y) = z$:

$$g_i f_i^{-1}f_j(z) - g_j(z) = u$$

c'est-à-dire :

$$f_i^{-1}f_j(z) - g_i^{-1}g_j(z) = u$$

équation devant avoir une solution et une seule en z .

l'automorphisme $g_j^{-1}g_i f_i^{-1}f_j$ doit donc être un orthomorphisme.

Par la suite, pour garder un mode de calcul qui soit toujours le même, nous associerons à :

$$\begin{cases} f_i(x_i) + f_j(x_j) = \alpha \\ g_i(x_i) + g_j(x_j) = \beta \end{cases}$$

l'automorphisme : $f_i^{-1} f_j \quad g_j^{-1} g_i$

c) D'une façon générale, il s'agit de chercher à quelle condition, k arrangements (T_k) isotopes - Do sont orthogonaux.

De même que les questions précédentes avaient déjà été étudiées, ce problème plus général a été envisagé par Monsieur Maurin ([6]) pour la construction de tableaux orthogonaux.

Soient : $[x_1, x_2, \dots, x_k ; \theta_1^i(x_1) + \theta_2^i(x_2) + \dots + \theta_k^i(x_k)]$

$x_j \in X$, $j \in [1, k]$, $i \in [1, k]$,

les k -arrangements (T_k) isotopes - Do.

(Rappelons que X est toujours un groupe abélien noté additivement et que $\theta_j^i (\forall i) , (\forall j)$ est un automorphisme de X sur X).

Par définition, les k -arrangements (T_k) isotopes-Do sont orthogonaux si tout système de t équations à t inconnues , $t \in [2, k]$ extrait du système I suivant a une solution et une seule :

$$I \quad \begin{cases} \theta_1^1(x_1) + \theta_2^1(x_2) + \dots + \theta_k^1(x_k) = a^1 \\ \dots \\ \theta_1^k(x_1) + \theta_2^k(x_2) + \dots + \theta_k^k(x_k) = a^k \end{cases}$$

Par applications du théorème 1 de la page 81 (ou ce qui revient au même par tout procédé consistant à éliminer une variable), on peut ramener l'étude de l'orthogonalité des k arrangements (T_k) à l'étude de l'orthogonalité d'arrangements $(T)_{k-1}$. Le système I peut s'écrire :

$$II \quad \begin{cases} (\theta_i^j)^{-1} \theta_1^j(x_1) + (\theta_i^j)^{-1} \theta_2^j(x_2) + \dots + x_i + \dots \\ + (\theta_i^j)^{-1} \theta_k^j(x_k) = a^j \\ \forall j \in [1, k]. \end{cases}$$

Retranchons de chaque équation l'équation (h), on obtient :

$$\text{III} \quad \left\{ \begin{array}{l} \left[(\theta_i^j)^{-1} \theta_1^j - (\theta_i^h)^{-1} \theta_1^h \right] (x_1) + \dots + \left[(\theta_i^j)^{-1} \theta_k^j - (\theta_i^h)^{-1} \theta_k^h \right] (x_k) = a^j - a^h \\ \forall j \in [1, k], \quad j \neq h, \end{array} \right.$$

système qui peut s'écrire par changement de variables :

$$\left\{ \begin{array}{l} y_1 = (\theta_i^h)^{-1} \theta_1^h(x_1) \\ y_2 = (\theta_i^h)^{-1} \theta_2^h(x_2) \\ \dots \\ y_k = (\theta_i^h)^{-1} \theta_k^h(x_k). \end{array} \right.$$

$$\text{IV} \quad \left\{ \begin{array}{l} \left[(\theta_1^h)^{-1} (\theta_i^h) (\theta_i^j)^{-1} \theta_1^j - I \right] (y_1) + \dots + \left[(\theta_k^h)^{-1} (\theta_i^h) (\theta_i^j)^{-1} \theta_k^j - I \right] (y_k) = a_1^j - a_1^h \\ \forall j \in [1, k], \quad j \neq h \end{array} \right.$$

Soit en abrégé :

$$\left\{ \begin{array}{l} \sum_{l=1}^k \left[(\theta_l^h)^{-1} \theta_i^h (\theta_i^j)^{-1} \theta_l^j - I \right] (y_l) = a_1^j - a_1^h \\ l \neq i \\ \forall j \in [1, k], \quad j \neq h. \end{array} \right.$$

Pourvu que les automorphismes :

$$(\theta_1^h)^{-1} \theta_i^h (\theta_i^j)^{-1} \theta_1^j, \quad \forall i \in [1, k], \quad \forall h \in [1, k], \quad \forall j \in [1, k],$$

$j \neq h$, $\forall l \in [1, k]$, $l \neq i$, soient des orthomorphismes, on a ramené l'étude de l'orthogonalité d'arrangements (T_k) à l'étude de l'orthogonalité d'arrangements $(T)_{k-1}$.

(A remarquer que cette condition exprime le fait que le système de deux équations (h) et (j) à deux inconnues x_i et x_1 doit avoir une solution et une seule, ce qui est requis dans le cas présent).

C'est ce premier résultat qui guide Monsieur Maurin dans son compte rendu ([6]) vers la notion de "résultant" associé à un système de k équations à k inconnues :

Définitions des Résultants ([6])

- Pour un système :

$$\begin{cases} f_1(x_1) + f_2(x_2) = \alpha \\ g_1(x_1) + g_2(x_2) = \beta \end{cases}$$

dont la matrice est :

$$\begin{bmatrix} f_1 & f_2 \\ g_1 & g_2 \end{bmatrix}$$

le résultant associé est l'automorphisme : $f_1^{-1} f_2 g_2^{-1} g_1$.

On a vu que le système proposé admet une solution et une seule si et seulement si $f_1^{-1} f_2 g_2^{-1} g_1$ est un orthomorphisme, c'est-à-dire, si l'endomorphisme :

$f_1^{-1} f_2 g_2^{-1} g_1 - I = \widehat{f_1^{-1} f_2 g_2^{-1} g_1}$ est un automorphisme.
(I représentant l'application identique).

- Plus généralement, soit le système :

$$\begin{cases} \sum_{j=1}^k \theta_j^i (x_j) = a^i \\ \forall i \in [1, k] \end{cases}$$

la matrice du système étant :

$$(\theta_j^i) = \begin{bmatrix} \theta_1^1 & \theta_2^1 & \dots & \theta_k^1 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^k & \theta_2^k & \dots & \theta_k^k \end{bmatrix}$$

Si l'on suppose l'existence de résultants associés à toute matrice carrée $[k-1 \times k-1]$ extraite de (θ_j^i) on va associer

à (θ_j^i) des résultants de la façon suivante :

On choisit deux couples d'indices quelconques (i_1, i_2) et (j_1, j_2) , $(i_1 \neq i_2, j_1 \neq j_2)$.

On considère des résultants des quatre matrices carrées d'ordre $k-1$ obtenues en biffant la $i^{\text{ème}}$ ligne et la $j^{\text{ème}}$ colonne de la matrice (θ_j^i) , $\forall i \in [i_1, i_2]$, $\forall j \in [j_1, j_2]$.

On obtient ainsi par exemple, quatre résultants notés :

$$R_{j_1}^{i_1}, R_{j_2}^{i_1}, R_{j_1}^{i_2}, R_{j_2}^{i_2}$$

On leur associe :

$$\widehat{R}_{j_1}^{i_1}, \widehat{R}_{j_2}^{i_1}, \widehat{R}_{j_1}^{i_2}, \widehat{R}_{j_2}^{i_2} \quad (\widehat{R}_j^i = R_j^i - I)$$

Dans ces conditions, un résultant de la matrice (θ_j^i) s'écrit :

$$(\widehat{R}_{j_2}^{i_2})^{-1} (\widehat{R}_{j_1}^{i_2}) (\widehat{R}_{j_1}^{i_1})^{-1} (\widehat{R}_{j_2}^{i_1})$$

pourvu que $(R_j^i) \quad \forall i \in [i_1, i_2] \quad \forall j \in [j_1, j_2]$ soit un orthomorphisme.

On voit que ce calcul de résultant dépend à chaque étape du choix de quatre indices. Si ce choix peut être g nant dans l' tude d'un syst me de k  quations   k inconnues, il n'a aucune importance dans le cas pr sent o  l'on s'int resse   l'orthogonalit  de k arrangements (T_k) et o  tous les résultants que l'on peut construire doivent  tre des orthomorphismes.

Le r sultat g n ral sera donc le suivant :

Th or me 7. ([6])

Les k arrangements (T_k) isotopes - Do :

$$[x_1, x_2, \dots, x_k, \theta_1^i(x_1) + \theta_2^i(x_2) + \dots + \theta_k^i(x_k)]$$

$$x_j \in X \quad \forall j \in [1, k] \quad , \quad \forall i \in [1, k]$$

-(X étant un groupe abélien et θ_j^i un automorphisme $\forall (i, j) \in [1, k]^2$)-

sont orthogonaux si et seulement si tous les résultants que l'on peut construire à partir de la matrice des θ_j^i sont des orthomorphismes.

Exemple de calcul d'un résultant.

Soit :

$$\begin{bmatrix} \theta_1^1 & \theta_2^1 & \theta_3^1 \\ \theta_1^2 & \theta_2^2 & \theta_3^2 \\ \theta_1^3 & \theta_2^3 & \theta_3^3 \end{bmatrix} = (\theta_j^i)$$

Prenons : $i_1 = j_1 = 2$, $i_2 = j_2 = 3$.

$$\begin{bmatrix} R_2^2 & R_3^2 \\ R_2^3 & R_3^3 \end{bmatrix} = \begin{bmatrix} (\theta_1^1)^{-1} \theta_3^1 (\theta_3^3)^{-1} \theta_1^3 & (\theta_1^1)^{-1} \theta_2^1 (\theta_2^3)^{-1} \theta_1^3 \\ (\theta_1^1)^{-1} \theta_3^1 (\theta_3^2)^{-1} \theta_1^2 & (\theta_1^1)^{-1} \theta_2^1 (\theta_2^2)^{-1} \theta_1^2 \end{bmatrix}$$

D'où :

$$\begin{bmatrix} \widehat{R_3^3} & \widehat{R_2^3} \\ \widehat{R_3^2} & \widehat{R_2^2} \end{bmatrix} = \begin{Bmatrix} [(\theta_1^1)^{-1} \theta_2^1 (\theta_2^2)^{-1} \theta_1^2 - I] & [(\theta_1^1)^{-1} \theta_3^1 (\theta_3^2)^{-1} \theta_1^2 - I] \\ [(\theta_1^1)^{-1} \theta_2^1 (\theta_2^3)^{-1} \theta_1^3 - I] & [(\theta_1^1)^{-1} \theta_3^1 (\theta_3^3)^{-1} \theta_1^3 - I] \end{Bmatrix}$$

et un résultant de (θ_j^i) :

$$[(\theta_1^1)^{-1} \theta_2^1 (\theta_2^2)^{-1} \theta_1^2 - I]^{-1} [(\theta_1^1)^{-1} \theta_3^1 (\theta_3^2)^{-1} \theta_1^2 - I]$$

$$[(\theta_1^1)^{-1} \theta_3^1 (\theta_3^3)^{-1} \theta_1^3 - I]^{-1} [(\theta_1^1)^{-1} \theta_2^1 (\theta_2^3)^{-1} \theta_1^3 - I]$$

(si $\widehat{R_3^3}$, $\widehat{R_2^3}$, $\widehat{R_3^2}$, $\widehat{R_2^2}$, sont des automorphismes).

IV. Exemples de construction de réseaux (R).

1) Rappelons tout d'abord un résultat élémentaire de la théorie des Groupes.

Un groupe abélien G non cyclique dont l'ordre est une puissance d'un nombre premier : p^m est le produit direct de groupes cycliques sans élément commun (excepté l'élément neutre).

Si les ordres de ces sous-groupes cycliques sont p^{m_1} , p^{m_2} , ..., p^{m_k} avec

$$m = \sum_{i=1}^k m_i, \quad ,$$

on dira que le groupe G est de type $(m_1, m_2, \dots, m_k)$. Par convention : $m_1 \geq m_2 \geq \dots \geq m_k$.

Un groupe abélien G de type $(1, 1, \dots, 1)$ et d'ordre p^m est donc le produit de groupes cycliques élémentaires d'ordre p . Considérons alors un groupe G d'ordre p^m et de type $(1, 1, \dots, 1)$. Soit G_1 un sous-groupe de G d'ordre p^{m-1} . Le réseau (R) correspondant sera construit de la façon suivante :

Les points du réseau seront identifiés aux sous-groupes d'ordre p de G n'appartenant pas à G_1 .

Les plans du réseau seront identifiés aux sous-groupes d'ordre p^{m-1} de G différents de G_1 .

La Relation d'incidence sera la relation d'inclusion d'un sous-groupe dans un autre.

Il est facile de vérifier que l'on a ainsi obtenu un réseau (R) en calculant ses constantes :

- Nombre de points du réseau :

$$n = \frac{p^m - 1}{p - 1} - \frac{p^{m-1} - 1}{p - 1} = p^{m-1}$$

- Nombre de plans du réseau passant par un point (nombre de classes) :

$$N = 1 + p + p^2 + \dots + p^{m-2}$$

- Nombre de plans du réseau :

$$Np.$$

- Nombre de plans du réseau passant par deux points :

$$1 + p + p^2 + \dots + p^{m-3}$$

La construction effectuée est très connue puisqu'elle correspond à la construction d'une géométrie Euclidienne :

$E G [p, k-1]$ et que le réseau (R) se confond avec cette géométrie.

2) Soient maintenant deux groupes, un groupe G_1 abélien d'ordre p^n et de type $(1, 1, \dots, 1)$, un groupe G_2 abélien d'ordre q^n et de type $(1, 1, \dots, 1)$.

Considérons alors le groupe G d'ordre $p^n q^n$ produit de G_1 par G_2 .

Otons de ce groupe G deux sous-groupes :

- un groupe G_3 d'ordre $p^{n-1} q^n$
- un groupe G_4 d'ordre $p^n q^{n-1}$

Intéressons-nous alors aux sous-groupes de G suivants :

- les sous-groupes d'ordre pq non inclus dans G_3 ou dans G_4 ,
- les sous-groupes d'ordre $p^{n-1} q^{n-1}$ non inclus dans G_3 ou dans G_4 .

Nous allons voir que l'on en déduit l'existence d'un réseau (R) dont les points sont identifiés aux sous-groupes d'ordre pq et les plans sont identifiés aux

sous-groupes d'ordre $p^{n-1} q^{n-1}$, la relation R d'incidence étant la relation d'inclusion d'un sous-groupe dans un autre.

Pour établir ce résultat, il suffit d'effectuer les calculs suivants :

a) Nombre de plans.

Il suffit de calculer le nombre de sous-groupes d'ordre $p^{n-1} q^{n-1}$ non inclus dans $G_3 \cup G_4$.

D'où :

$$\frac{p^n - 1}{p - 1} \cdot \frac{q^n - 1}{q - 1} - \frac{q^n - 1}{q - 1} - \frac{p^n - 1}{p - 1} + 1 = pq \left[\frac{p^{n-1} - 1}{p - 1} \frac{q^{n-1} - 1}{q - 1} \right]$$

$$\text{Nombre de plans} = pq \left[\frac{p^{n-1} - 1}{p - 1} \frac{q^{n-1} - 1}{q - 1} \right]$$

b) Nombre de points.

Il suffit de calculer le nombre de sous-groupes d'ordre pq non inclus dans $G_3 \cup G_4$:

d'où :

$$\frac{q^n - 1}{q - 1} \frac{p^n - 1}{p - 1} - \frac{q^n - 1}{q - 1} \frac{p^{n-1} - 1}{p - 1} - \frac{q^{n-1} - 1}{q - 1} \frac{p^n - 1}{p - 1} + \frac{q^{n-1} - 1}{q - 1} \frac{p^{n-1} - 1}{p - 1} =$$

$$\left[= (pq)^{n-1} \right]$$

$$\text{Nombre de points} : (pq)^{n-1}.$$

c) Nombre de plans dans une classe.

Un sous-groupe d'ordre $p^{n-1} q^{n-1}$ non inclus dans $G_3 \cup G_4$ intersecte G_3 suivant un sous-groupe d'ordre $p^{n-2} q^{n-1}$, G_4 suivant un sous-groupe d'ordre $p^{n-1} q^{n-2}$, et le sous-groupe $G_3 \cap G_4$ suivant un sous-groupe d'ordre $p^{n-2} q^{n-2}$. Une classe de plans est alors définie par l'ensemble

de sous-groupes d'ordre $p^{n-1} q^{n-1}$ contenant un sous-groupe d'ordre $p^{n-2} q^{n-2}$ de $G_3 \cap G_4$, n'appartenant ni à G_3 ni à G_4 .

Il y en a : $n - n_1 - n_2 + 1$ avec:

$$n = \frac{p^n - p^{n-2}}{p^{n-1} - p^{n-2}} \frac{q^n - q^{n-2}}{q^{n-1} - q^{n-2}} = pq + p + q + 1$$

$$n_1 = \frac{p^{n-1} - p^{n-2}}{p^{n-1} - p^{n-2}} \frac{q^n - q^{n-2}}{q^{n-1} - q^{n-2}} = q + 1$$

$$n_2 = \frac{p^n - p^{n-2}}{p^{n-1} - p^{n-2}} \frac{q^{n-1} - q^{n-2}}{q^{n-1} - q^{n-2}} = p + 1$$

Il y a donc pq plans dans chaque classe.

d) Nombre de plans passant par deux points : t .

Ce nombre bien sûr dépend des deux points considérés. Dans le cas le plus défavorable :

$$t = \frac{p^{n-2} - 1}{p - 1} \frac{q^{n-2} - 1}{q - 1}.$$

3) La généralisation de la construction précédente est immédiate.

On considère k groupes abéliens G_i d'ordre p_i^n et de type $(1, 1, \dots, 1)$.

Soit le groupe produit $G = G_1 \times G_2 \dots \times G_k$.

Soient $G^{(i)}$ k sous-groupes de G d'ordre $p_1^n \dots p_i^{n-1} \dots p_k^n$.

On s'intéresse alors d'une part aux sous-groupes de G d'ordre $p_1^{n-1} p_2^{n-1} \dots p_k^{n-1}$ non inclus dans

$$\bigcup_{i=1}^k G^{(i)}$$

d'autre part, aux sous-groupes de G d'ordre $p_1 p_2 \dots p_k$ non inclus dans

$$\bigcup_{i=1}^k G^{(i)}.$$

Aux premiers, on fait correspondre les plans du réseau.

Aux seconds, on associe les points du réseau, la relation d'incidence étant toujours la relation d'inclusion d'un sous-groupe dans un autre.

Le calcul des constantes du réseau ainsi construit est alors le même que précédemment.

$$\text{- Nombre total de plans : } p_1 p_2 \dots p_k \left[\frac{p_1^{n-1}-1}{p_1-1} \frac{p_2^{n-1}-1}{p_2-1} \dots \frac{p_k^{n-1}-1}{p_k-1} \right]$$

$$\text{- Nombre total de points : } (p_1 p_2 \dots p_k)^{n-1}$$

$$\text{- Nombre de plans dans une classe : } p_1 p_2 \dots p_k.$$

$$\text{- Nombre maximum de plans passant par 2 points :}$$

$$\prod_{i=1}^k \left(\frac{p_i^{n-2}-1}{p_i-1} \right)$$

V. Exemples de constructions de réseaux (R) dans le cas des Corps de Galois. ([7] et [8]) :

1) Construction de réseaux (R)_t.

a) Introduction.

Il a déjà été remarqué (à propos du schéma d'association des P.B.I.B.D.) que lorsque $\text{Card } [X] = p^n$, p étant un nombre premier, les réseaux (R) peuvent être des familles de plans extraites d'une géométrie Euclidienne à k dimensions. X est alors le corps de Galois à $q = p^n$ éléments.

Le problème de construction des réseaux (R)_t se ramène alors au problème suivant : construire une famille de plans extraite d'une Géométrie projective PG $[k-1, p^n]$ telle que par tout point ne passent pas plus de t hyperplans.

De nombreuses constructions peuvent dès lors être envisagées. Nous en donnerons une utilisant la connaissance des quadriques dans une géométrie projective.

b) Quadriques dans une géométrie projective.

- Soit dans une géométrie projective PG $[k; p^n]$ la surface (S) donnée par son équation : $f(x_1 \ x_2 \ \dots \ x_{k+1}) = 0$.

L'équation du plan tangent en $(x_1 \ x_2 \ \dots \ x_k)$ à cette surface est :

$$\sum_{i=1}^{k+1} x_i f'x_i = 0 \quad \text{avec } f(x_1 \ x_2 \ \dots \ x_{k+1}) = 0.$$

L'équation d'un plan tangent issu d'un point $M(x_1^0 \ \dots \ x_{k+1}^0)$ à cette surface est :

$$\sum_{i=1}^{k+1} (x_i - x_i^0) f'x_i = 0$$

avec :

$$f(x_1 \ x_2 \ \dots \ x_{k+1}) = 0.$$

Le plan polaire d'un point $(x_1^0, x_2^0, \dots, x_{k+1}^0)$ a pour équation :

$$\sum_{i=1}^{k+1} x_i f'x_i^0 = 0$$

L'intersection de ce plan polaire avec la surface étant donnée par :

$$\begin{cases} \sum_{i=1}^{k+1} x_i f'x_i^0 = 0 \\ f(x_1 \ x_2 \ \dots \ x_{k+1}) = 0. \end{cases}$$

- Soit $x = (x_1 \ x_2 \ \dots \ x_{k+1})$ un point de la géométrie projective PG $[k ; p^n]$.

Une quadrique Q dans cette géométrie aura pour équation $x A x' = 0$.

A étant une matrice triangulaire de $k+1$ lignes et de $k+1$ colonnes, x' désignant le vecteur transposé de x .

Si la caractéristique de $GF(p^n)$ est différent de 2, Q peut s'écrire : $x B x' = 0$.

B étant une matrice symétrique $(k+1, k+1)$. Sinon cela est impossible.

Nous gardons donc l'écriture $x A x' = 0$ comme équation d'une quadrique.

En appliquant les notions élémentaires que nous venons de rappeler, on a pour :

l'équation du plan tangent en x à la quadrique Q :

$$x(A + A') X' = 0 \quad \text{avec } x A x' = 0$$

(A' étant la matrice transposée de A).

l'équation d'un plan tangent issu de x^0 à la quadrique Q :

$$x(A + A') (X' - x'_0) = 0 \quad \text{avec } x A x' = 0$$

l'équation du plan polaire de x_0 :

$$x_0(A + A') x' = 0.$$

Rappelons encore que deux points α et β sont conjugués par rapport à la quadrique si :

$$\alpha(A + A') \beta' = 0$$

Les points coïncidant avec leur propre conjugué sont donc : les points de Q si la caractéristique du corps est différent de 2, tous les points de la géométrie dans le cas contraire.

Enfin, une quadrique Q sera dégénérée si on peut l'écrire par un changement de variables approprié : $x C x' = 0$.

C étant une matrice $(k+1, k+1)$ triangulaire ne contenant que des 0 dans sa dernière ligne et sa dernière colonne.

- Primrose a montré que toute quadrique non dégénérée dans une PG $[2k ; p^n]$ contient des variétés linéaires de dimension $k-1$ sans contenir de variétés de dimension plus élevée.

Il n'y a donc qu'un seul type de quadrique dans une géométrie PG $[2k ; p^n]$.

Mais dans une géométrie PG $[2k-1 ; p^n]$ deux cas peuvent se présenter :

α) le cas des quadriques hyperboliques (quadriques de type 1).

Ce sont des quadriques contenant des variétés linéaires de $k-1$ dimensions sans en contenir de dimension plus grande.

β) Le cas des quadriques elliptiques (quadriques de type 2).

Ce sont des quadriques contenant des variétés linéaires de $k-2$ dimensions sans en contenir de dimension plus grande.

Du point de vue combinatoire Primrose donne les résultats suivants :

Nombre de points d'une Quadrique.

$$A) \text{ PG } [2k ; p^n] , n_{2k}^0 = \frac{(p^n)^{2k-1}}{p^n - 1}$$

$$B) \text{ PG } [2k-1 ; p^n]$$

$$\left\{ \begin{array}{l} \text{Quadriques hyperboliques (type 1)} : n_{2k-1}^1 = \frac{[(p^n)^{k-1}] [(p^n)^{k-1} + 1]}{p^n - 1} \\ \text{Quadriques elliptiques (type 2)} : n_{2k-1}^2 = \frac{[(p^n)^{k+1}] [(p^n)^{k-1} - 1]}{p^n - 1} \end{array} \right.$$

avec $k \geq 2$

avec $k \geq 2$

c) Construction de réseaux $(R)_t$.

Pour construire un réseau $(R)_t$, nous allons considérer la famille des plans tangents à une quadrique non dégénérée.

Pour connaître t , il sera nécessaire de connaître le nombre maximum de plans tangents à la quadrique passant par un point quelconque.

Il est facile de voir que ce nombre est égal au nombre de points communs de la quadrique avec le plan polaire du point considéré.

On est donc ramené à étudier l'intersection d'une quadrique avec la famille des plans polaires des points de la géométrie et à chercher le nombre maximum des points possibles.

Ces points communs sont donnés par :

$$\begin{cases} x_0 (A + A') x' = 0 \\ x A x' = 0 \end{cases}$$

Si x_0 est le point fixé.

Deux cas sont à examiner a priori :

A) x_0 est un point de la quadrique Q .

On a alors aux points communs de l'intersection :

$$\begin{cases} x_0 (A + A') x' = 0 \\ x_0 A x'_0 = 0 \\ x A x' = 0. \end{cases}$$

On est donc ramené à compter le nombre des points communs d'une quadrique et de son plan tangent en un point quelconque.

B) x_0 n'est pas sur la quadrique Q .

Et on est ramené à compter le nombre des points communs d'une quadrique avec un plan quelconque non tangent.

Cas A

Le plan tangent en un point quadrique de $PG[k ; p^n]$ a en commun avec cette dernière un cône de la géométrie $PG[k-1 ; p^n]$.

Le nombre des génératrices de ce cône est le même que le nombre de points d'une quadrique de la géométrie $PG[k-2 ; p^n]$ soit n_{k-2}^x .

Sur chaque génératrice du cône, d'autre part, il y a p^n points autres que le sommet.

D'où le nombre de points du cône :

$$p^n n_{k-2}^x + 1$$

($x = 0, 1, 2$ suivant la dimension de la géométrie et le type de la quadrique considérée).

Cas B

L'intersection d'un plan non tangent avec une quadrique dans la géométrie $PG[k ; p^n]$ est une quadrique de la géométrie $PG[k-1 ; p^n]$.

- En résumé peuvent donc se présenter les cas suivants pour le nombre de plans tangents issus d'un point à une quadrique :

(∞) Géométrie : $PG[2k ; p^n]$

$$\left\{ \begin{array}{l} - p^n n_{2k-2}^0 - 2 + 1 \\ - n_{2k-3}^1 \\ - n_{2k-3}^2 \end{array} \right.$$

$$\beta) \text{ Géométrie PG } [2k-1 ; p^n]$$

$$\left\{ \begin{array}{l} \text{- Quadrique de type 1 : } \begin{cases} p^n n_{2k-3}^1 + 1 \\ n_{2k-2}^0 \end{cases} \\ \text{- Quadrique de type 2 : } \begin{cases} p^n n_{2k-3}^2 + 1 \\ n_{2k-2}^0 \end{cases} \end{array} \right.$$

Il est facile de démontrer les inégalités :

$$p^n n_{2k-3}^1 + 1 > n_{2k-2}^0 > p^n n_{2k-3}^2 + 1$$

$$n_{2k-3}^1 > p^n n_{2k-2}^0 + 1 > n_{k-3}^2$$

Donc :

$$\alpha) \text{ Géométrie PG } [2k ; q] : t = n_{2k-3}^1 = \frac{(q^{k-1}-1)(q^{k-1}-1)}{(q-1)}$$

$$\beta) \text{ Géométrie PG } [2k-1 ; q]$$

$$\left\{ \begin{array}{l} \text{Quadrique de type 1 : } t = q n_{2k-3}^1 + 1 = \frac{q [q^{k-1}-1] [q^{k-2}+1]}{q-1} + 1 \\ \text{Quadrique de type 2 : } t = n_{2k-2}^0 = \frac{q^{2k-2}-1}{q-1} \end{array} \right.$$

Les réseaux $(R)_t$ sont donc entièrement décrits, puisque l'on connaît le nombre de plans tangents à une quadrique non dégénérée. Il est égal au nombre de points de la quadrique.

D'où les résultats :

		N: nombre de classes de plans	t: nombre maximum de plans passant par deux points	Card [E]: nombre de points du réseau
$PG [2k; q]$		n_{2k}^0	n_{2k-3}^1	q^{2k+1}
$PG [2k-1; q]$	type 1	n_{2k-1}^1	$qn_{2k-3}^1 + 1$	q^{2k}
	type 2	n_{2k-1}^2	n_{2k-2}^0	q^{2k}

2) Construction de réseaux $(R)_{k-1}$.

Soit un réseau $(R) = (E, F, F_i, i \in I, R, k, q)$.
 On considère toujours le cas où $E = X^{k-1}$ avec $X = GF(q)$ $q = p^n$
 p premier. Il s'agit donc comme on l'a déjà vu, si l'on
 désire obtenir des réseaux $(R)_{k-1}$, de construire des familles
 de plans issues d'une géométrie projective à $k-1$ dimensions
 $PG [k-1; p^n]$ telles que par tout point de cette géométrie,
 il ne passe pas plus de $k-1$ plans. On a alors le résultat
 suivant :

Théorème 1 ([11])

Dans la géométrie projective $PG [k-1; p^n]$ la famille
 de plans suivante :

$$\left\{ \begin{array}{l} x_1 + x_2 \alpha + x_3 \alpha^2 + \dots + x_k \alpha^{k-1} = 0 \\ \forall \alpha \in GF(q = p^n) \\ \text{et :} \\ x_k = 0 \end{array} \right.$$

est telle que par tout point de la géométrie, il ne passe

pas plus de $k-1$ plans. ($p^n > k$)

Démonstration.

La démonstration de ce théorème est d'un type bien connu puisqu'elle utilise les propriétés des déterminants de Van der Monde :

Le déterminant :

$$\begin{vmatrix} 1 & \alpha_{i_1}^1 & \dots & \alpha_{i_1}^{k-1} \\ 1 & \alpha_{i_2}^1 & \dots & \alpha_{i_2}^{k-1} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha_{i_k}^1 & \dots & \alpha_{i_k}^{k-1} \end{vmatrix} = \prod_{i \neq j} (\alpha_i - \alpha_j)$$

est différent de zéro pourvu que : $\alpha_{i_1} \neq \alpha_{i_2} \neq \dots \neq \alpha_{i_k}$. Dans ces conditions, si l'on considère $k-1$ plans, on pourra extraire du système correspondant de $k-1$ équations un déterminant de Van der Monde à $k-1$ lignes et $k-1$ colonnes différent de 0 et on aura ainsi défini un point et un seul (rappelons que les coordonnées d'un point sont ici homogènes puisque l'on est dans une géométrie projective). Le fait d'ajouter le plan $x_k = 0$ ne change absolument rien au résultat, puisque :

$$\begin{vmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & \alpha_1 & \dots & \alpha_1^{k-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_{k-2} & \dots & \alpha_{k-2}^{k-1} \end{vmatrix} = (-1)^{k+1} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

Corollaire 1.

Il existe un réseau $(R)_{k-1}$ de $q+1$ familles de q plans parallèles extrait d'une géométrie Euclidienne à k dimensions

EG $[k ; q] :$

$$\left\{ \begin{array}{l} x_1 + x_2 \alpha + \dots + x_k \alpha^{k-1} = a \\ \forall \alpha \in \text{GF}(q) \\ \forall a \in \text{GF}(q) \\ \text{et :} \\ x_k = a \quad \forall a \in \text{GF}(q). \end{array} \right.$$

$(q > k).$

En utilisant l'équivalence entre réseaux $(R)_{k-1}$ et arrangements (T_k) orthogonaux, on peut énoncer le théorème suivant :

Théorème 2.

Dans le cas où $X = \text{GF}(q)$, $q > k$, on sait construire une famille de $q+1-k$ arrangements (T_k) orthogonaux sur $X : [x_1 \ x_2 \ \dots \ x_k ; a \ \alpha]$ avec :

$$a \alpha = \sum_{h=0}^{k-2} x_{h+1} \left[\frac{\prod_{i \neq h} f_i(\alpha)}{\prod_{i \neq h} f_i(\alpha_h)} \right] + x_k \left[\frac{k-1}{\prod_{i=0}^{k-1}} f_i(\alpha) \right]$$

$$\forall \alpha \in \text{GF}(q)$$

$$\alpha \neq \alpha_i \quad \forall i \in [0, k-1] \quad \alpha_0 = 0, \quad \alpha_i \neq \alpha_j \quad \forall (i, j)$$

$$f_i(\alpha) = \alpha - \alpha_i.$$

Démonstration. Il suffit de procéder à une série de changement de variables.

La famille :

$$\left\{ \begin{array}{l} x_1 + x_2 \alpha + \dots + x_k \alpha^{k-1} = 0 \\ \alpha \in \text{GF}(q) \\ x_k = 0. \end{array} \right.$$

peut s'écrire :

$$\left\{ \begin{array}{l} x_1 \prod_{i \neq 0} (\alpha - \alpha_i) + x_2 \prod_{i \neq 1} (\alpha - \alpha_i) + \dots + x_{h+1} \prod_{i \neq h} (\alpha - \alpha_i) + \\ \dots + x_k \prod_{i=0}^{k-1} (\alpha - \alpha_i) = 0 \\ \forall \alpha \neq \alpha_i \\ x_1 = 0 \\ x_2 = 0 \\ \vdots \\ x_k = 0 \end{array} \right.$$

et ceci si $\alpha_0 = 0, \alpha_1, \alpha_2, \dots, \alpha_{k-1}$ sont k éléments différents de $\text{GF}(q)$.

En posant : $f_i(\alpha) = \alpha - \alpha_i$ et en normant, on obtient finalement la famille de plans :

$$\left\{ \begin{array}{l} x_1 \prod_{i \neq 0} f_i(\alpha) + \dots + x_{h+1} \frac{\prod_{i \neq h} f_i(\alpha)}{\prod_{i \neq h} f_i(\alpha_h)} + \dots + x_k \prod_{i=0}^{k-1} f_i(\alpha) = 0 \\ x_h = 0 \quad \forall h \in [1, k] \end{array} \right.$$

d'où le résultat.

Richesse des familles obtenues.

Le problème général est le suivant :

Le nombre de symboles q de X et la dimension k étant fixés, quelle est la valeur maximum de N nombre d'arrangements (T_k) orthogonaux que l'on peut construire sur X ?

On dira qu'une famille de tels arrangements est complète si N atteint la valeur maximum.

Nous avons donc ce problème à étudier ici dans le cas où $X = \text{GF}(q)$.

Théorème 3.

La famille d'arrangements (T_k) construite au théorème 2 est complète si et seulement si :

Pour toute valeur de $(a_0, a_1, \dots, a_{k-1})$ on peut trouver

(1) soit $k-1$ valeurs distinctes de t dans $GF(q)$

telles que :

$$a_{k-1} - a_{k-2} \sum t_i + \dots + (-1)^h a_{k-1-h} \sum t_{i_1} t_{i_2} \dots t_{i_h} + \dots + (-1)^{k-1} a_0 t_1 t_2 \dots t_{k-1} = 0$$

(2) Soit $k-2$ valeurs distinctes de t dans $GF(q)$

telles que :

$$a_{k-2} - a_{k-3} \sum t_i + \dots + (-1)^h a_{k-2-h} \sum t_{i_1} t_{i_2} \dots t_{i_h} + \dots + (-1)^{k-2} a_0 t_1 t_2 \dots t_{k-2} = 0$$

Démonstration.

Soit la famille de plans précédents :

$$\begin{cases} x_1 + t x_2 + \dots + t^{k-1} x_k = a \\ t \in GF(q) \quad , \quad a \in GF(q) \\ x_k = a \quad , \quad a \in GF(q) \end{cases}$$

Est-il possible d'ajouter un plan :

$$a_0 x_1 + a_1 x_2 + \dots + a_{k-1} x_k = \infty$$

en conservant un réseau $(R)_{k-1}$

On devra avoir :

$$D_1 = \begin{vmatrix} a_0 & a_1 & \dots & a_{k-1} \\ 1 & t_1 & \dots & t_1^{k-1} \\ \dots & & & \\ 1 & t_{k-1} & \dots & t_{k-1}^{k-1} \end{vmatrix} \neq 0$$

et :

$$D_2 = \begin{vmatrix} a_0 & a_1 & \dots & a_{k-1} \\ 1 & t_1 & \dots & t_1^{k-1} \\ \dots & & & \\ 1 & t_{k-2} & \dots & t_{k-2}^{k-1} \\ 0 & 0 & \dots & 1 \end{vmatrix} \neq 0$$

pour $k-1$ valeurs de t distinctes.

Si par contre, il existait $k-1$ valeurs de t distinctes telles que $D_1 = 0$ ou bien $k-2$ valeurs de t distinctes telles que $D_2 = 0$, la famille de plans du théorème 2 serait complète.

Or :

$$D_1 = \prod_{i \neq j} (t_i - t_j) \left[a_{k-1} - a_{k-2} \sum t_i + a_{k-3} \sum t_i t_j + \dots + (-1)^h a_{k-1-h} \sum t_{i_1} t_{i_2} \dots t_{i_h} + \dots + (-1)^{k-1} a_0 t_1 t_2 \dots t_{k-1} \right]$$

et :

$$D_2 = \prod_{i \neq j} (t_i - t_j) \left[a_{k-2} - a_{k-3} \sum t_i + a_{k-4} \sum t_i t_j + \dots + (-1)^{k-2} a_0 t_1 t_2 \dots t_{k-2} \right]$$

D'où le résultat annoncé.

REFERENCES

- [1]- Guérin : Existence et propriétés des carrés latins orthogonaux. Thèse.
- [2]- Stein : Homogeneous quasi-groups. Pacific J. Math 14. (1964) 1091-1102.
- [3]- H.B. Mann : On orthogonal Latin squares. Bull. of the Amer. Math. Society. 50 (1944) 249-257.
- [4]- H.B. Mann : The construction of sets of orthogonal Latin Squares. A. M. S. vol. 13 (1942) 418-423.
- [5]- Johnson-Dulmage-Mendelsohn : Orthomorphisms of abelian groups and orthogonal latin squares. Canad. J. Math. 13 (1961) 356-372.
- [6]- F. Maurin : Automorphismes propres de groupes. C. R. Acad. Sc. Paris t 262 (23 mai 1966) p. 1194-1197.
- [7]- Primrose : Quadrics in finite geometries. Proc. Cambridge Phil. Soc. 47 (1951). 299-304.
- [8]- D. K. Ray Chaudhuri : Some results on quadrics in finite geometry. Canad. J. Math. 1962. p. 123
- [9]- Stein : On the fondations of quasi-groups. Trans. A. M. S. vol. 85. 1957. p.228-256.
- [10]- Bruck : Some results in the theory of quasi-groups Trans. A. M. S. vol. 55. 1944. p.19-52
- [11]- I. M. Chakravarti : Séminaire I. S. U. P. 9 avril 1962.

C H A P I T R E I V

Réseaux Cycliques et Codes Cycliques

I. Introduction.

L'étude des codes cycliques n'est pas nouvelle et de nombreux chercheurs y ont contribué.

Nous nous proposons seulement de voir comment à partir de la notion de réseau géométrique, l'on peut rejoindre ce grand centre d'intérêt de la théorie des codes correcteurs d'erreurs.

Nous aboutirons assez rapidement à un langage très classique et ne dégagerons en conséquence aucun résultat nouveau.

II. Définition des Réseaux Cycliques et des Codes Cycliques

1) Définition des Réseaux Cycliques.

Soit un réseau $(E, F, F_i, i \in [1, N], q, k)$. Nous avons vu au chapitre II comment il était possible d'associer un code à ce réseau.

A chaque point x de l'ensemble E , on faisait correspondre le mot du code suivant :

$$\begin{aligned}\psi(x) &= [\psi_1(x), \psi_2(x), \dots, \psi_N(x)] \\ &= \psi \circ f(x) = [\psi_1 \circ f_1(x), \psi_2 \circ f_2(x), \dots, \\ &\quad \psi_N \circ f_N(x)]\end{aligned}$$

- f_i désignant l'application faisant correspondre à x le plan de la classe i passant par x , $\forall i \in [1, N]$
- ψ_i étant une bijection de F_i sur X , ensemble de q éléments, $\forall i \in [1, N]$.

Dans ces conditions, le réseau $(E, F, F_i, i \in [1, N], q, k)$ est un réseau cyclique, si et seulement si, pour tout point x de l'ensemble E , il existe un point x' de E et un seul, tel que :

$$I \quad \left\{ \begin{array}{l} \psi_1(x') = \psi_2(x) \\ \psi_2(x') = \psi_3(x) \\ \dots \\ \psi_{N-1}(x') = \psi_N(x) \\ \psi_N(x') = \psi_1(x) \end{array} \right.$$

Justification de la définition.

Si la définition d'un réseau cyclique était la suivante : "Pour tout point x de E , il existe un point x' de E , au moins, tel que les relations I soient vérifiées", cela entraînerait la définition proposée ci-dessus à savoir que le point x est unique. En effet, si l'on supposait par l'absurde qu'il existe deux tels points x'_1 et x'_2 , on aurait :

$$\left\{ \begin{array}{l} \psi_1(x'_1) = \psi_1(x'_2) = \psi_2(x) \\ \dots \\ \psi_{N-1}(x'_1) = \psi_{N-1}(x'_2) = \psi_N(x) \\ \psi_N(x'_1) = \psi_N(x'_2) = \psi_1(x) \end{array} \right.$$

Or, ceci est contraire à l'axiome de tout codage énoncé au chapitre II : $\forall (x'_1, x'_2) \in E^2, x'_1 \neq x'_2,$

$$\exists i \in [1, N] \implies \psi_i(x'_1) \neq \psi_i(x'_2)$$

Si un réseau est cyclique, on peut donc définir une application α de E dans E telle que :

$$x \xrightarrow{\alpha} x' = \alpha(x),$$

et :

$$\text{II} \quad \left\{ \begin{array}{l} \psi_1 [\alpha(x)] = \psi_2(x) \\ \psi_2 [\alpha(x)] = \psi_3(x) \\ \dots \\ \psi_{N-1} [\alpha(x)] = \psi_N(x) \\ \psi_N [\alpha(x)] = \psi_1(x) \end{array} \right.$$

L'application α ainsi définie est une bijection de E sur E .

En effet, elle est injective ainsi qu'on l'a vu dans la justification de la définition d'un réseau cyclique (si α n'était pas injective, il pourrait exister deux points de E conduisant au même mot du code et l'axiome de codage ne serait pas satisfait).

D'autre part, on montre facilement que α est surjective en utilisant les propriétés II.

En effet, soit x' un point de E et soit : $[\psi_1(x'), \psi_2(x'), \dots, \psi_N(x')]$ le mot du code correspondant à x' .

Considérons $\alpha(x')$. On a :

$$\left\{ \begin{array}{l} \psi_1 [\alpha(x')] = \psi_2(x') \\ \vdots \\ \psi_{N-1} [\alpha(x')] = \psi_N(x') \\ \psi_N [\alpha(x')] = \psi_1(x') \end{array} \right.$$

Considérons alors $\alpha[\alpha(x')] = \alpha^2(x')$. On a de la même façon :

$$\left\{ \begin{array}{l} \psi_1 [\alpha^2(x')] = \psi_3 (x') \\ \psi_2 [\alpha^2(x')] = \psi_4 (x') \\ \dots \\ \psi_{N-2} [\alpha^2(x')] = \psi_N (x') \\ \psi_{N-1} [\alpha^2(x')] = \psi_1 (x') \\ \psi_N [\alpha^2(x')] = \psi_2 (x') \end{array} \right.$$

et ainsi de suite. Finalement :

$$\left\{ \begin{array}{l} \psi_1 [\alpha^{N-1}(x')] = \psi_N (x') \\ \psi_2 [\alpha^{N-1}(x')] = \psi_1 (x') \\ \dots \\ \psi_N [\alpha^{N-1}(x')] = \psi_{N-1}(x') \end{array} \right.$$

En posant : $x = \alpha^{N-1}(x')$, on obtient les relations I

$$\left\{ \begin{array}{l} \psi_1 (x) = \psi_N (x') \\ \psi_2 (x) = \psi_1 (x') \\ \dots \\ \psi_N (x) = \psi_{N-1} (x') \end{array} \right.$$

Autrement dit $\forall x' \in E$, on vient de construire x tel que : $\alpha(x) = x'$; α est donc une application surjective.

De façon analogue, les relations II permettent d'écrire :

$$\psi_1 [\alpha^2(x)] = \psi_2 [\alpha(x)] = \psi_3(x)$$

puis :

$$\psi_1 [\alpha^3(x)] = \psi_2 [\alpha^2(x)] = \psi_3 [\alpha(x)] = \psi_4(x)$$

..

et enfin :

$$\psi_1 [\alpha^N(x)] = \psi_1(x).$$

Si le réseau est cyclique, le mot du code que l'on peut lui associer et correspondant à $x \in E$:

$[\psi_1(x), \psi_2(x), \dots, \psi_N(x)]$ peut donc s'écrire :

$\{\psi_1(x), \psi_1[\alpha(x)], \dots, \psi_1[\alpha^{N-1}(x)]\}$, sachant que $\alpha^N = I$

(I désignant l'application identique). Réciproquement, on vérifie que cette propriété entraîne **que** le réseau est cyclique.

On a donc le résultat suivant :

Théorème 1.

Le réseau $(E, F, F_i, i \in [1, N], q, k)$ est cyclique si et seulement s'il existe une surjection ψ de E dans X , ensemble de q éléments, et une bijection α de E sur E telles que :

$$\alpha^N = I$$

I désignant l'application identique et que tout mot du code correspondant au réseau puisse s'écrire :

$$\forall x \in E : \{ \psi(x), \psi[\alpha(x)], \psi[\alpha^2(x)], \dots, \psi[\alpha^{N-1}(x)] \}$$

2) Définition des codes cycliques.

Soit le code $(N, k) : (\mathcal{C}; f_i, i \in [1, N])$, formé des mots :

$$[f_1(x), f_2(x), \dots, f_N(x)] = [a_1, a_2, \dots, a_N]$$

$$\forall x \in \mathcal{C}, \text{Card}[\mathcal{C}] = q^k, f_i(x) \in X, \forall i \in [1, N],$$

$\text{Card}[X] = q$. (On emploie les notations du chapitre II).

Le code (N, k) sera un code cyclique si et seulement si l'appartenance du mot $[a_1, a_2, \dots, a_N]$ au code entraîne l'appartenance du mot $[a_2, a_3, \dots, a_N, a_1]$ au même code.

On a alors le théorème suivant :

Théorème 2.

L'existence d'un réseau cyclique entraîne l'existence d'un code cyclique.

Ce résultat découle directement des définitions précédentes des réseaux cycliques et des codes cycliques et de l'énoncé du théorème 1.

Remarque.

Il y a lieu de remarquer que la connaissance d'un code (N, k) n'implique nullement l'existence d'un réseau (R) . Le théorème 2 n'admet pas de réciproque en conséquence. Il faudrait autrement imposer aux applications f_i , $i \in [1, N]$ de $\mathcal{C}$ dans X des propriétés permettant de justifier les propriétés de définition des réseaux (c.f. Chapitre I). Par contre, le théorème 1 s'applique aux codes cycliques, vue sa démonstration. Son énoncé légèrement modifié devient :

Théorème 3.

Le code $(N, k) = (\mathcal{C}; f_i, i \in [1, N])$ est cyclique si et seulement s'il existe une application f de $\mathcal{C}$ dans X et une bijection α de $\mathcal{C}$ sur $\mathcal{C}$ telles que : $\alpha^N = I$

et que tout mot du code correspondant à x de $\mathcal{C}$ s'écrit :

$$\{f(x), f[\alpha(x)], \dots, f[\alpha^{N-1}(x)]\}$$

III. Etude algébrique des réseaux cycliques quand $X = GF(q)$.

1) Introduction.

Dans le paragraphe précédent, nous avons constaté que réseau cyclique ou code cyclique pouvaient être étudiés de façon analogue, vues leurs définitions, certaines propriétés de définition des réseaux devant être justifiées dans le cas de l'étude des réseaux cycliques.

Nous nous proposons dans ce paragraphe de rappeler quelques résultats concernant l'étude des codes cycliques quand on peut munir X d'une structure de corps de Galois.

Nous constaterons que cette étude s'applique aussi bien aux réseaux cycliques et que nous sommes dans un cas particulier où il y a équivalence entre ces deux recherches.

Nous verrons que l'on peut définir les codes cycliques aussi bien que les réseaux cycliques par des équations de récurrence (ce qui est connu depuis longtemps (références [1] et [2])).

Nous compléterons cette étude par quelques calculs qui nous permettront de dégager des résultats analogues à ceux de la référence [3].

2) Etude algébrique des réseaux cycliques.

Soit un réseau cyclique $(E, F, F_i, i \in [1, N], q, k)$. D'après le théorème 1 du paragraphe II précédent, il existe une surjection ψ de E dans X , ensemble de q éléments et une bijection α de E sur E , telle que $\alpha^N = I$ et telles que

tout mot du code cyclique correspondant au réseau puisse s'écrire :

$$\forall x \in E : \{ \psi(x) , \psi[\alpha(x)] , \dots \psi[\alpha^{N-1}(x)] \}$$

Nous allons nous placer, dans la suite du chapitre, dans le cas particulier suivant :

- X est muni d'une structure de corps de Galois $GF(q)$. ($q = p^n$, p premier).
- E est un espace vectoriel de dimension k sur le corps X.
- α est un automorphisme de E sur E, tel que $\alpha^N = I$.
- ψ est une forme linéaire de E sur X.

Il convient d'examiner en premier lieu l'axiome de tout codage pour voir s'il n'introduit pas de restrictions sur α et ψ .

a) Axiome de codage.

α) L'axiome de tout codage s'écrit dans le cas présent :

$$\forall (x_1, x_2) \in E^2, x_1 \neq x_2, \exists i \in [1, N] \Rightarrow \psi_i f_i(x_1) \neq \psi_i f_i(x_2)$$

c'est-à-dire :

$$\forall (x_1, x_2) \in E^2, x_1 \neq x_2, \exists i \in [0, N-1] \Rightarrow \psi[\alpha^i(x_1)] \neq \psi[\alpha^i(x_2)]$$

c'est-à-dire :

$$\psi[\alpha^i(x_1 - x_2)] \neq 0$$

Ce qui s'écrit :

$$\bigcap_{i \in [0, N-1]} \text{Ker } [\Psi[\alpha^i]] = 0$$

$\text{Ker}(\Psi\alpha^i)$ désignant le noyau de $\Psi\alpha^i$, c'est-à-dire l'ensemble des éléments x de E tels que : $\Psi[\alpha^i(x)] = 0$.

$$\beta) \text{ Soit } N \text{ le noyau de } \Psi : \\ x \in N \iff \Psi(x) = 0.$$

Soit S un sous-espace invariant de α dans E :

$$\alpha(S) \subset S.$$

Supposons alors $S \subset N$. Nous allons voir que l'axiome de codage est alors en défaut.

En effet, soient x_1 et x_2 deux éléments distincts de S . On a :

$$\Psi[\alpha^i(x_1)] = \Psi[\alpha^i(x_2)] = 0 \quad \forall i \in [0, N-1]$$

Donc :

$$x_1 - x_2 \in \text{Ker } [\Psi(\alpha^i)] \quad , \quad \forall i \in [0, N-1]$$

Et ceci est impossible.

On doit donc nécessairement avoir : $S \not\subset N$

Supposons donc maintenant : $S \not\subset N$, et ceci pour tout sous-espace invariant S de α dans E .

Il est facile de démontrer que dans ces conditions, le codage est correct.

Effectivement, soit x un élément quelconque, mais différent de 0, de $S \cap N$.

Il est impossible que $\psi(x)$, $\psi[\alpha(x)]$, ..., $\psi[\alpha^{N-1}(x)]$ soient tous nuls.

En effet, soit r la dimension S ; $S \cap N$ est alors de dimension $r-1$.

x , $\alpha(x)$, ..., $\alpha^{r-1}(x)$ sont linéairement indépendants et engendrent S : autrement dit $\alpha^i(x)$ par exemple n'appartient pas à $S \cap N$ et :

$$\psi[\alpha^i(x)] \neq 0.$$

($S \cap N$ n'est pas un sous-espace invariant de α , en résumé).
D'où le théorème suivant :

Théorème 1 (réf. [2]).

Pour que le codage soit correct, il faut et il suffit que les sous-espaces invariants de α dans E ne soient pas contenus dans le noyau de ψ .

Cette condition étant remplie, nous allons chercher à caractériser le code cyclique $\mathcal{C}$ correspondant au réseau cyclique :

$$\{\psi(x), \psi[\alpha(x)], \dots, \psi[\alpha^{N-1}(x)]\}, \forall x \in E.$$

b) Caractérisation d'un Code Cyclique.

(α) Nous commencerons par le rappel d'un résultat élémentaire d'algèbre linéaire.

Soit E un espace vectoriel de dimension n sur un corps X et F un sous-espace vectoriel de E de dimension d . On sait que l'on peut trouver une base de E , soit $e_1, e_2, \dots, e_n$ telle que $e_1, e_2, \dots, e_d$ soit une base de F . Considérons alors le sous-ensemble F° du dual de E , soit E^* , suivant :

$$F^\circ = \{u : u \in E^*, u(x) = 0, \forall x \in F\}$$

Puisque l'on a : $u(x) = 0$, on a $u(e_i) = 0$, $\forall i \in [1, d]$
 Autrement dit, u est de la forme suivante :

$$u = \sum_{i=d+1}^n \eta_i e_i^*$$

(où $\eta_i = u(e_i)$ et où e_1^* , e_2^* , ..., e_n^* désigne la base duale de E^* , associée à e_1 , e_2 , ..., e_n ; c'est-à-dire telle que :

$$e_i^*(e_j) = \delta_{ij} \quad , \quad \delta_{ij} = \begin{cases} 1, & \text{si } i = j \\ 0, & \text{si } i \neq j \end{cases}$$

Réciproquement, toute forme linéaire u pouvant s'écrire :

$$\sum_{i=d+1}^n \eta_i e_i^*$$

appartient à F^0 .

F_0 est donc un sous-espace vectoriel de E^* de dimension $n-d$.

Cas particulier.

Soit $u_\alpha \in E^*$, $\alpha \in A$, $\text{Card } [A] \geq n$, une famille de formes linéaires de E dans X telle que :

$$\bigcap_{\alpha \in A} \text{Ker } u_\alpha = 0$$

($\text{Ker } u_\alpha$ désignant le noyau de u_α)

Alors les formes linéaires u_α engendrent le dual E^* de E .

(β) Soit maintenant $\mathcal{C}$ le code cyclique associé au réseau cyclique précédent.

$\mathcal{C}$ est un sous-espace vectoriel de X^N espace vectoriel à N dimensions.

Les applications ψ_α^i , $\forall i \in [0, N-1]$, en tant que

formes linéaires de E^* dual de E soumises à la contrainte :

$$\bigcap_{i \in [0, N-1]} \text{Ker } \Psi[\alpha^i] = 0 ,$$

engendrent E^* par application de la propriété α) précédente.

On peut alors remarquer que puisque E^* est de dimension k , les $k+1$ formes linéaires : Ψ , $\Psi\alpha$, ..., $\Psi\alpha^k$ ne peuvent pas être linéairement indépendantes.

Autrement dit $\Psi\alpha^k$ peut s'exprimer linéairement en fonction de Ψ , $\Psi\alpha$, ..., $\Psi\alpha^{k-1}$.

On a donc une relation :

$$\underline{\Psi c_0 + \Psi\alpha c_1 + \Psi\alpha^2 c_2 + \dots + \Psi\alpha^{k-1} c_{k-1} + \Psi\alpha^k = 0}$$

pour des valeurs fixes $c_0, c_1, \dots, c_{k-1}$ dans $\text{GF}(p^n)$.

On montre alors facilement (référence [2]) que le polynôme :

$$m(\alpha) = c_0 + c_1\alpha + \dots + c_{k-1}\alpha^{k-1} + \alpha^k$$

est le polynôme minimum de α (puisque $\alpha^N = I$, il est bien évident, d'autre part, que $m(\alpha) \mid \alpha^N - I$). Finalement, on peut énoncer le théorème suivant :

Théorème 2 (référence [2])

Le polynôme de degré k :

$$m(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{k-1}\alpha^{k-1} + \alpha^k$$

est le polynôme minimum de l'automorphisme α : c'est-à-dire que $m(\alpha)$ est le polynôme de plus bas degré, (dont le coefficient du terme en α^k est pris égal à l'unité) tel que $m(\alpha) = 0$.

On a en outre les propriétés suivantes :

- $m(\alpha)$ divise $\alpha^N - I$.

- L'automorphisme α de E sur E n'a aucun sous-espace invariant contenu dans le noyau de Ψ .

3) on vient de voir en particulier que :

$$\forall x \in E, \quad \psi[m(\alpha)(x)] \equiv 0,$$

c'est-à-dire, en développant :

$$\psi[(c_0 + c_1\alpha + \dots + c_{k-1}\alpha^{k-1} + \alpha^k)(x)] \equiv 0$$

ce qui s'écrit :

$$\sum_{i=0}^k c_i \psi[\alpha^i(x)] \equiv 0$$

Si l'on pose :

$$(a^0, a^1, a^2, \dots, a^{N-1}) = [\psi(x), \psi[\alpha(x)], \dots, \psi[\alpha^{N-1}(x)]]$$

On a donc :

$$\sum_{i=0}^k c_i a^i = 0$$

De la même façon, on a plus généralement :

$$\forall x \in E, \quad \forall j : \quad \psi\{m(\alpha)[\alpha^j(x)]\} \equiv 0$$

c'est-à-dire :

$$\sum_{i=0}^k c_i \psi[\alpha^{i+j}(x)] \equiv 0$$

(en n'oubliant pas que $\alpha^N = I$).

Donc :

$$\sum_{i=0}^k c_i a^{i+j} = 0 \quad \forall j \quad \begin{array}{l} \text{(avec } a^N = a^0) \\ \text{(} a^{N+1} = a^1 \dots \text{ etc...)} \end{array}$$

On peut donc énoncer le théorème suivant :

Théorème 3 (référence [1])

Soit $(a^0, a^1, \dots, a^{N-1})$ un mot quelconque d'un code (N, k) construit sur un alphabet X de q éléments.

Supposons que l'on puisse munir X d'une structure de Corps de Galois $GF(q)$ ($q = p^n$, p premier).

Le code (N, k) sera cyclique, si tout mot $(a^0, a^1, \dots, a^N)$ de ce code est solution de l'équation de récurrence:

$$\sum_{i=0}^k C_i a^{i+j} = 0, \quad ,$$

avec la convention $C_k = 1$ et $a^N = a^0$, $a^{N+1} = a^1$, etc ...

En outre, le polynôme $m(x) = C_0 + C_1 x + C_2 x^2 + \dots + C_{k-1} x^{k-1} + x^k$ doit diviser $x^N - 1$.

Remarque.

Le résultat du théorème 3, que l'on vient d'obtenir, permet donc de décrire un code cyclique par une équation linéaire de récurrence de type connu :

$$(1) \quad \sum_{i=0}^k C_i a^{i+j} = 0.$$

On peut remarquer, sans d'ailleurs utiliser la théorie de ces équations de récurrence linéaire que les codes cycliques ainsi obtenus correspondent à des réseaux cycliques.

En effet, l'équation (1) permet, pour $j = 0$, d'exprimer linéairement a^k en fonction de $a^0, a^1, \dots, a^{k-1}$. De même, plus généralement, elle permet d'exprimer a^i en fonction linéaire de $a^0, a^1, \dots, a^{k-1}$ et ceci pour tout $i \in [k, N-1]$.

Autrement dit, un mot quelconque du code peut s'écrire :

$$\left[a^0, a^1, \dots, a^{k-1}, \sum_{i=0}^{k-1} C_i a^i, \sum_{i=0}^{k-1} C_i^1 a^i, \dots, \sum_{i=0}^{k-1} C_i^{N-k} a^i \right]$$

les C_i^j étant fixés en valeur par l'équation (1). Le réseau (R) correspondant au code est alors constitué

- des q^k points suivants :

$$(a^0, a^1, \dots, a^{k-1}) \quad \forall (a^0, a^1, \dots, a^{k-1}) \in (GF(q))^k$$

- et des N classes de plans suivantes :

$$\left\{ \begin{array}{lll} a^0 = \alpha^0 & \forall \alpha^0 \in GF(q) & (1^\circ \text{ classe}) \\ a^1 = \alpha^1 & \forall \alpha^1 \in GF(q) & (2^\circ \text{ classe}) \\ \dots & & \\ a^{k-1} = \alpha^{k-1} & \forall \alpha^{k-1} \in GF(q) & (k^\circ \text{ classe}) \\ \sum_{i=0}^{k-1} C_i^k a^i = \alpha^k & \forall \alpha^k \in GF(q) & (k+1^\circ \text{ classe}) \\ \dots & & \\ \sum_{i=0}^{k-1} C_i^{N-k} a^i = \alpha^{N-1} & \forall \alpha^{N-1} \in GF(q) & (N^\circ \text{ classe}) \end{array} \right.$$

Il est facile de vérifier sur ces données, les propriétés de définition des réseaux (R). Il n'y a par contre aucune raison pour que l'on obtienne des réseaux ($\hat{R}$), ce que l'on aurait si toutes les constantes C_i^j étaient différentes de 0.

3) Quelques résultats classiques concernant l'étude des codes cycliques.

Nous nous bornerons à effectuer quelques calculs complémentaires conduisant à des résultats connus. Nous nous placerons toujours dans le cas III 2) d'un réseau cyclique $(E, F, F_i, i \in [1, N], q, k)$, où

- E est un espace vectoriel de dimension k sur le corps X, avec $X = GF(q)$, $q = p^n$, p premier.

- α est un automorphisme de E sur E , tel que :
 $\alpha^N = I$.

- ψ est une forme linéaire de E sur X .

Les résultats acquis aux théorèmes du paragraphe précédent III, 2) peuvent donc être utilisés.

a) Soit $m(x) = C_0 + C_1x + \dots + C_{k-1}x^{k-1} + x^k = 0$,

$C_0, C_1, \dots, C_{k-1} \in GF(q)$, le polynôme minimum de α .

Supposons $(N, p) = 1$ et soit $GF(q^m)$ le corps de décomposition des racines de $x^N - 1$.

α) Soit $(a^0, a^1, \dots, a^{N-1})$ un mot du code cyclique que l'on peut construire moyennant ces données, c'est-à-dire tel que :

$$\sum_{i=0}^k a^{i+j} C_i = 0 \quad \forall j.$$

On sait, par application de la théorie élémentaire des équations linéaires de récurrence que l'on a alors :

$$a^i = \sum_{j=1}^k \alpha_{ij} r_j^i, \quad \forall i \in [0, N-1]$$

$r_1, r_2, \dots, r_k$ étant les k racines de $m(x)$, (nécessairement distinctes puisque $(N, p) = 1$) dans $GF(q^m)$.

(Remarquons que α_{ij} comme r_j appartiennent à $GF(q^m)$ pour $\forall i, \forall j$ mais que a^i appartient à $GF(q)$).

Soit β une racine primitive de $GF(q^m)$.

On peut écrire :

$$r_h = \beta^{i_h} \quad \forall h \in [1, k].$$

(Le choix possible d'une autre racine primitive de $GF(q^m)$ est traité dans la référence [3] page 24).

On peut donc mettre a^i sous la forme suivante :

$$a^i = \alpha_{i1} (\beta^i)^{i1} + \alpha_{i2} (\beta^i)^{i2} + \dots + \alpha_{ik} (\beta^i)^{ik}$$

Soit alors :

$$\underline{H(u) = \alpha_{i1} u^{i1} + \alpha_{i2} u^{i2} + \dots + \alpha_{ik} u^{ik}}$$

On a :

$$\underline{a^i = H(\beta^i) \quad \forall i \in [0, N-1]}$$

Inversement soit :

$$H(u) = \sum_{j=1}^k \alpha_{ij} u^{ij}$$

$$\text{et } a^i = H(\beta^i) \quad , \quad \forall i \in [0, N-1]$$

Calculons :

$$\sum_{i=0}^{N-1} \beta^{-i_h i} H(\beta^i) \quad , \quad \forall h \in [1, k]$$

$$\begin{aligned} \sum_{i=0}^{N-1} \beta^{-i_h i} H(\beta^i) &= \sum_{j=1}^k \sum_{i=0}^{N-1} \alpha_{ij} \beta^{i(i_j - i_h)} \\ &= \sum_{j=1}^k \alpha_{ij} \left[\sum_{i=0}^{N-1} \beta^{i(i_j - i_h)} \right] \\ &= N \alpha_{ij} \end{aligned}$$

Vu que $(N, p) = 1$, l'élément N dans $GF(q)$ (N fois l'élément unité) admet un inverse et on a :

$$\alpha_{ih} = N^{-1} \sum_{i=0}^{N-1} \beta^{-i_h i} H(\beta^i) \quad \forall h \in [1, k]$$

des racines de $m_i(x)$.

On peut écrire :

$$r_j^{(i)} = (\beta_i)^{a(j)}, \quad \forall i \in [1, h], \quad \forall j \in [1, k]$$

Dans ces conditions, on a :

$$a_i^j = \alpha_1^{(i)} (\beta_i^{a(1)})^j + \dots + \alpha_{k_i}^{(i)} (\beta_i^{a(k_i)})^j$$

et :

$$a^j = \sum_{i=1}^h \left[\alpha_1^{(i)} (\beta_i^{a(1)})^j + \dots + \alpha_{k_i}^{(i)} (\beta_i^{a(k_i)})^j \right]$$

$$\forall j \in [0, N-1]$$

Soit en posant :

$$H_i(u_i) = \alpha_1^{(i)} u_i^{a(1)} + \dots + \alpha_{k_i}^{(i)} u_i^{a(k_i)} :$$

$$a_i^j = H_i(\beta_i^j)$$

et :

$$H(u_1, u_2, \dots, u_h) = \sum_{i=1}^h H_i(u_i) :$$

$$a^j = H \left[\beta_1^j, \beta_2^j, \dots, \beta_h^j \right], \quad \forall j \in [0, N-1]$$

On peut donc énoncer le théorème suivant complétant les résultats du théorème 4 :

Théorème 5.

Dans le cas où le polynôme minimum de $\mathcal{A}$, $m(x)$ est le produit de h polynômes irréductibles $m_i(x)$, $i \in [1, h]$, on peut associer à chaque mot $(a^0, a^1, \dots, a^{N-1})$ du code,

un polynôme :

$$H(u_1, u_2, \dots, u_h) = \sum_{i=1}^h H_i(u_i)$$

tel que :

$$- a^j = H(\beta_1^j, \beta_2^j, \dots, \beta_h^j), \quad \forall j \in [0, N-1]$$

β_i désignant une racine primitive de $GF(q^{k_i})$, $\forall i \in [1, h]$

$$- H_i(u_i) = \alpha_{1'}^{(i)} u_i^{a(1)} + \dots + \alpha_{k_i}^{(i)} u_i^{a(k_i)}$$

$$\text{si } m_i(x) = \prod_{j=1}^{k_i} (x - \beta_i^{a(j)})$$

$$(\alpha_j^{(i)} \in GF(q^{k_i}), \quad \forall j \in [1, k_i]).$$

b) Les deux théorèmes précédents font apparaître des paramètres α_j^i dans la forme des polynômes $H(u)$ et $H(u_1, u_2, \dots, u_h)$ considérés. Ils restent en ce sens encore imprécis.

Nous allons chercher maintenant à lever cette imprécision en trouvant des relations liant les valeurs de ces paramètres.

∞) Nous considérerons tout d'abord le cas particulier d'un polynôme $m(x)$ irréductible sur $GF(q)$ et de degré k , la longueur N du code étant prise égale à $q^k - 1$.

Le polynôme $m(x)$ divise donc $x^{q^k-1} - 1$.

Soit β une racine primitive de $GF(q^k)$. Les racines de $x^{q^k-1} - 1$ sont les éléments non nuls de $GF(q^k)$, c'est-à-dire $\beta^i \quad \forall i \in [0, q^k-2]$.

On sait que le polynôme $m(x)$ peut se mettre sous la forme suivante :

$$m(x) = \prod_{0 \leq j \leq k-1} (x - \beta^{i_1})^{q^j},$$

la valeur i_1 dépendant de la racine β choisie.

On a donc :

$$H(u) = \sum_{0 \leq j \leq k-1} \alpha_{i_1} q^j u^{i_1 q^j}$$

comme forme pour le polynôme $H(u)$ correspondant à un certain mot du code : $(a^0, a^1, \dots, a^{N-1})$.

Dès lors :

$$N \alpha_{i_1} q^j = \sum_{i=0}^{N-1} \beta^{-i_1 q^j i} a_i$$

et :

$$\begin{aligned} N \alpha_{i_1} q^{j+1} &= \sum_{i=0}^{N-1} \beta^{-i_1 q^{j+1} i} a_i \\ &= \sum_{i=0}^{N-1} (\beta^{-i_1 q^j i})^q a_i^q \end{aligned}$$

(puisque $a_i^q = a_i$, $\forall a_i \in GF(q)$).

Finalement :

$$N \alpha_{i_1} q^{j+1} = \left(\sum_{i=0}^{N-1} \beta^{-i_1 q^j i} a_i \right)^q$$

et on a :

$$\alpha_{i_1 q^{j+1}} = (\alpha_{i_1 q^j})^q \quad \forall j$$

D'où les relations :

$$\begin{cases} \alpha_{i_1 q} = (\alpha_{i_1})^q \\ \alpha_{i_1 q^2} = (\alpha_{i_1})^{q^2} \\ \dots \\ \alpha_{i_1 q^{k-1}} = (\alpha_{i_1})^{q^{k-1}} \end{cases}$$

De sorte que le polynôme $H(u)$ peut s'écrire :

$$H(u) = \sum_{0 \leq j \leq k-1} (\alpha_{i_1} u^{i_1})^{q^j}$$

Remarques.

(1) - On obtiendra les q^k mots du code en faisant varier α_{i_1} dans $GF(q^k)$.

(2) - $H(u)$ se présente comme la trace de l'élément $\alpha_{i_1} u^{i_1}$ de $GF(q^k)$ sur $GF(q)$, soit $T(\alpha_{i_1} u^{i_1})$.

On peut, en résumé, énoncer le résultat suivant :

Théorème 6 .

Dans le cas où $m(x)$ est un polynôme irréductible de degré k et où la longueur N du code est égale à $q^k - 1$, le polynôme $H(u)$ que l'on peut associer à chaque mot du code est la trace d'un certain élément de $GF(q^k)$ (correspondant au mot du code et à la racine primitive β de $GF(q^k)$ choisis) sur $G(q)$: $T(\alpha_{i_1} u^{i_1}) = H(u)$.

β) Ce résultat très particulier peut tout d'abord être généralisé immédiatement au cas d'un code de longueur $N = q^{ks} - 1$, quand le polynôme $m(x)$ est toujours irréductible et de degré k .

$$m(x) = \prod_{0 \leq j \leq k-1} (x - \beta^{i_1 q^j}) \quad , \quad \beta \in GF(q^k)$$

Soit $n = \frac{q^{ks} - 1}{q^k - 1}$ et soit γ une racine primitive de $GF(q^{ks})$.

β racine primitive de $GF(q^k)$ peut être choisie telle que :

$$\underline{\gamma^n = \beta .}$$

On a alors :

$$m(x) = \prod_{0 \leq j \leq k-1} (x - \gamma^{ni_1} q^j)$$

et :

$$H(u) = \sum_{0 \leq j \leq k-1} (\alpha_{i_1} u^{i_1})^{q^j}, \alpha_{i_1} \text{ et } u \in \text{GF}(q^k),$$

polynôme que l'on associe à chaque mot du code peut également s'écrire :

$$H_1(v) = \sum_{0 \leq j \leq k-1} (\alpha'_{i_1} v^{i_1})^{nq^j}$$

$$v \text{ et } \alpha'_{i_1} \in \text{GF}(q^{sk}).$$

La trace $T(\alpha'_{i_1} u^{i_1})$ de l'élément $\alpha'_{i_1} u^{i_1}$ de $\text{GF}(q^k)$

sur $\text{GF}(q)$ peut donc également s'écrire en utilisant $\text{GF}(q^{sk})$ corps de décomposition des racines de $x^{q^{sk}-1}$:

$$T(\alpha'_{i_1} v^{i_1})^n$$

α'_{i_1} et v^{i_1} étant des éléments de $\text{GF}(q^{sk})$.

Il n'y a finalement aucune différence avec le cas traité en α) si ce n'est une période de longueur q^{k-1} dans chaque mot du code, période qui se trouve répétée n fois.

Remarque.

Ces deux cas particuliers ont déjà été examinés (c.f. référence [3]). On peut démontrer que les codes obtenus sont optima, en étudiant le nombre de racines de $T(\alpha'_{i_1} u^{i_1})$ dans $\text{GF}(q^k)$ ce qui déterminera la norme

de chaque mot du code. La norme (c.f. Chapitre II) d'un mot quelconque des codes ainsi décrits peut d'ailleurs être retrouvée directement par utilisation des résultats précédents du paragraphe III.

Considérons en effet le réseau cyclique correspondant au code.

$m(\alpha)$ est irréductible et de degré k .

Pour tout point x de E (différent de $(0, 0, \dots, 0)$), $x, \alpha(x), \alpha^2(x), \dots, \alpha^{q^k-2}(x)$ sont différents.

D'autre part, le noyau de ψ' est un sous-espace vectoriel de E de dimension $k-1$, donc sur les q^{k-1} valeurs successives de $\psi[\alpha^i(x)]$, $i \in [0, q^k-2]$, $q^{k-1}-1$ sont nulles, d'où $q^k - q^{k-1}$ composantes du mot non nulles répétées chacune $n = \frac{q^{sk}-1}{q^{k-1}}$ fois.

D'où enfin, la norme d'un mot du code correspondant à x :

$$n(q^k - q^{k-1})$$

(résultat de la référence [3] page 29)

γ) Nous considérerons enfin le cas d'un polynôme $m(x)$ produit de h polynômes $m_i(x)$ de degré k_i , irréductibles sur $GF(q)$, avec

$$\sum_{i=1}^h k_i = k :$$

$$m(x) = \prod_{i=1}^h m_i(x)$$

Nous prendrons comme longueur du code : $N = q^{ks}-1$ et ferons nos calculs dans le corps de décomposition des racines de $m(x)$, soit $GF(q^k)$.

Soit β une racine primitive de $GF(q^k)$. On a :

$$m_i(x) = \prod_{0 \leq j \leq k_i-1} (x - \beta^{a(i)q^j})$$

et :

$$m(x) = \prod_{i=1}^h \left[\prod_{j=0}^{k_i-1} (x - \beta^{a(i)q^j}) \right]$$

Dans ces conditions, le polynôme :

$$H(u) = \alpha_{i_1} u^{i_1} + \alpha_{i_2} u^{i_2} \dots + \alpha_{i_k} u^{i_k}$$

qui correspond au mot $(a^0, a^1, \dots, a^{N-1})$ du code avec :

$$a^i = \alpha_{i_1} \beta^{i_1 i} + \alpha_{i_2} \beta^{i_2 i} + \dots + \alpha_{i_k} \beta^{i_k i}$$

peut s'écrire, en utilisant le résultat du théorème 4 :

$$H(u) = \sum_{i=1}^h \left[\sum_{j=0}^{k_i-1} \alpha_{a(i)q^j} u^{a(i)q^j} \right]$$

Cherchons maintenant les relations pouvant lier les valeurs de $\alpha_{a(i)q^j}$.

On a vu (Théorème 4) que :

$$N \alpha_{i_h} = \sum_{i=0}^{N-1} \beta^{-i_h i} a^i$$

ce qui s'écrit dans le cas présent :

$$N \alpha_{a(i)q^j} = \sum_{k=0}^{N-1} \beta^{-a(i)q^j k} a^k$$

De même :

$$\begin{aligned} N \alpha_{a(i)q^{j+1}} &= \sum_{k=0}^{N-1} \beta^{-a(i)q^{j+1} k} a^k \\ &= \left[\sum_{k=0}^{N-1} \left(\beta^{-a(i)q^j k} a^k \right) \right] q \end{aligned}$$

Donc :

$$\alpha_{a(i)q^{j+1}} = \left[\alpha_{a(i)q^j} \right]^q, \quad \forall i \in [1, h].$$

D'où les relations :

$$\begin{cases} \alpha_{a(i)q} = \left[\alpha_{a(i)} \right]^q \\ \alpha_{a(i)q^2} = \left[\alpha_{a(i)} \right]^{q^2} \\ \dots \\ \alpha_{a(i)q^{k_i-1}} = \left[\alpha_{a(i)} \right]^{q^{k_i-1}} \end{cases}$$

et finalement :

$$(1) \quad H(u) = \sum_{i=1}^h \left[\sum_{j=0}^{k_i-1} (\alpha_{a(i)} u^{a(i)})^{q^j} \right]$$

avec $\alpha_{a(i)} \in GF(q^k)$ et $u^{a(i)} \in GF(q^k)$.

Nous allons nous servir du théorème 5 et des deux cas particuliers α) et β) traités précédemment pour préciser ce résultat.

Les polynômes $m_i(x)$ étant irréductibles, on a vu qu'il leur correspondait une décomposition de l'espace vectoriel E en sous-espaces vectoriels invariants dans l'automorphisme α . On a vu que :

$$E = \bigcup_{i=1}^h S_i \quad \text{avec } S_i \cap S_j = 0,$$

S_i étant l'espace invariant correspondant à $m_i(x)$.

Tout point $x \neq 0$ de E pouvait s'écrire :

$$x = \sum_{i=1}^h x_i \quad \text{avec } x_i \in S_i$$

De la même façon que dans la démonstration du théorème 5, faisons jouer à S_i le rôle de E . Le polynôme minimum de α est alors $m_i(x)$ et on a :

$$m_i(x) = \prod_{j=0}^{k_i-1} (x - \beta_i^{a'(i)q^j}) ,$$

β_i étant une racine primitive de $GF(q^{k_i})$.

D'après les deux cas particuliers que l'on vient d'étudier en α) et β), on sait que le polynôme $H_i(u_i)$ correspondant à $x_i \in S_i$, s'écrira :

$$H_i(u_i) = \sum_{j=0}^{k_i-1} \left[\alpha_{a'(i)} u^{a'(i)} \right]^{q^j}$$

avec $\alpha_{a'(i)}$ et $u_i \in GF(q^{k_i})$.

Ceci est, bien sûr, valable pour tout $i \in [1, h]$.

En utilisant enfin le théorème 5, on voit que le polynôme $H(u_1, u_2, \dots, u_h)$ que l'on peut associer à un élément x quelconque de E , donc à un mot quelconque $(a^0, a^1, \dots, a^{N-1})$ du code, est le suivant :

$$(2) \quad H(u_1, u_2, \dots, u_h) = \sum_{i=1}^h H_i(u_i) = \sum_{i=1}^h \left[\sum_{j=0}^{k_i-1} \left[\alpha_{a'(i)} u^{a'(i)} \right]^{q^j} \right]$$

Cette formule précise le résultat obtenu à la formule (1).

Remarque.

Le vecteur code $(a^0, a^1, \dots, a^{N-1})$ correspondant à $H(u_1, \dots, u_h)$ est tel que :

$$a^i = H(\beta_1^i, \beta_2^i, \dots, \beta_h^i), \quad \forall i \in [0, N-1]$$

β_j étant une racine primitive de $GF(q^{k_j})$, $\forall j \in [1, h]$.

On obtient donc bien :

$$q^{k_1} \times q^{k_2} \times \dots \times q^{k_h} = q^k$$

mots dans le code.

Le polynôme $H_i(u_i)$ étant la trace de l'élément $\alpha_{a^i(i)} u_i^{a^i(i)}$ de $GF(q^{k_i})$ sur $GF(q)$, $H(u_1, u_2, \dots, u_h)$ se présente donc comme la somme des traces de h éléments $\alpha_{a^i(i)} u_i^{a^i(i)}$ de $GF(q^{k_i})$ sur $GF(q)$ $\forall i \in [1, h]$.

Signalons enfin qu'en choisissant les racines primitives $\beta_1, \beta_2, \dots, \beta_h$ telles que :

$$\beta_i = \gamma^{n_i} \quad \forall i \in [1, h]$$

avec γ racine primitive de $GF(q^k)$ et $n_i = \frac{q^{k_i}-1}{q^k-1}$, $\forall i \in [1, h]$

le polynôme $H(u_1, u_2, \dots, u_h)$ peut s'écrire :

$$(3) \quad H(u) = \sum_{i=1}^h \left[\sum_{j=0}^{k_i-1} (\alpha_{a^i(i)} u^{a^i(i)})^{n_i q^j} \right]$$

avec : $\alpha_{a^i(i)}$ et $u^{a^i(i)} \in GF(q^k)$.

En résumé, on peut énoncer le théorème suivant :

Théorème 7.

Dans le cas où $m(x)$ est le produit de h polynômes irréductibles $m_i(x)$ de degré k_i , $\sum k_i = k$ et où la longueur N du code est égale à $q^{sk}-1$, le polynôme $H(u_1, u_2, \dots, u_h)$ que l'on peut associer à chaque mot

du code est le suivant :

$$H(u_1, u_2, \dots, u_h) = \sum_{i=1}^h T_i \left[\alpha_{a'(i)} u_i^{a'(i)} \right]$$

$T_i \left[\alpha_{a'(i)} u_i^{a'(i)} \right]$ désignant la trace de l'élément $\alpha_{a'(i)} u_i^{a'(i)}$ de $GF(q^{k_i})$ sur $GF(q)$.

Remarque.

Le problème consistant à calculer la norme d'un mot du code est donc ramené au problème du nombre de racines de $H(u)$ dans $GF(q^k)$ (en utilisant (3)).

c) Nous nous bornerons ici quant à l'étude des codes cycliques puisque les calculs effectués vont conduire à des théorèmes connus.

A propos des calculs précédents, il en existe d'autres présentations utilisant le fait qu'un code cyclique est un idéal dans l'algèbre des polynômes modulo $x^N - 1$.

REFERENCES.

- [1] - W.W. Peterson. Error Correcting Codes. Wiley 1962.
- [2] - Assmus. Mattson. Error Correcting Codes : An axiomatic approach. Information and Control, Vol 6, N° 4, December 1963.
- [3] - P. Camion. Codes Correcteurs d'Erreurs. Revue CETHEDC 3ème trimestre 1966.

A N N E X E

Les deux chapitres suivants constituent deux possibilités d'étude des mêmes problèmes que précédemment.

Le premier chapitre est consacré à l'étude de la notion nouvelle de Systèmes de Plans, le deuxième chapitre à l'étude des treillis correspondant aux Réseaux et aux Systèmes de Plans.

Nous verrons que les treillis associés aux Réseaux sont difficiles à construire alors qu'il est facile de trouver des exemples de treillis isomorphes à des systèmes de Plans. (Malheureusement, cela ne nous permet pas de construire des arrangements (T_k) , les Systèmes de Plans devant pour cela vérifier une propriété, la propriété (P) définie au chapitre V, qui est très difficilement maniable).

Ces deux chapitres ne conduisent donc pas à des résultats significativement supérieurs aux précédents, mais l'on y envisage l'étude des arrangements (T_k) et des réseaux, sous une optique différente de celle du chapitre I.

Ce sont toutes ces raisons qui nous ont conduits à repousser ces deux chapitres dans une Annexe.

C H A P I T R E V

Systèmes de Plans et Réseaux Associés.

I. Introduction.

La notion de systèmes de Droites a été introduite par R.C. Bose et utilisée par Guérin en vue de construire des familles de quasi-groupes mutuellement orthogonaux sur un ensemble E. Après avoir rappelé les définitions et les théorèmes de R.C. Bose concernant les systèmes de Droites tels qu'ils sont exposés dans la thèse de Monsieur Guérin, nous généraliserons cette étude en donnant une définition des Systèmes de Plans que nous appliquerons au problème de la construction d'arrangements (T_k) orthogonaux sur un ensemble X de q éléments.

Nous définirons ensuite certaines structures de réseaux que l'on peut associer à l'étude des réseaux (R).

II. Systèmes de Droites (références [1] , [2] , [4]).

1) - Définition des Systèmes de Droites.

Soient deux ensembles E et F et R un sous-ensemble de $E \times F$ vérifiant les propriétés suivantes :

$$\text{a) } \forall (x_1, x_2, y_1, y_2) \in E^2 \times F^2, \quad \forall (i, j) \in \{1, 2\}^2. \\ (x_i, y_j) \in R \implies x_1 = x_2 \quad \text{ou} \quad y_1 = y_2$$

$$\text{b) } \forall (x_1, x_2) \in E^2, \quad \exists y \in F, \quad (x_1, y) \in R, \quad (x_2, y) \in R.$$

On appelle système de Droites un système constitué par un triplet (E, F, R) vérifiant a) et b).

Si on appelle points les éléments de E et droites les éléments de F, on peut définir une relation d'appartenance $\in$ (ou relation d'incidence) entre les points et les droites. C'est la suivante :

$$x \in y \iff (x, y) \in R.$$

Un système de Droites est alors constitué par un triplet (E, F, R) vérifiant :

(1) Deux points quelconques sont incidents à une droite et à une seule.

Ce qui entraîne que deux droites quelconques sont incidentes à au plus un point.

Dans toute la suite, on identifiera et c'est légitime F à une famille de parties de E, $(x, y) \in R$, signifiant rappelons-le que le point x appartient à la droite y.

Un sous-ensemble K de F sera un faisceau si et seulement si :

$$(A) : \forall (D_1, D_2) \in K^2, D_1 \neq D_2, D_1 \cap D_2 = \emptyset$$

$$(B) : \forall x \in E, \exists D \in F, (x, D) \in R$$

Si K ne vérifie que (A), ce sera un faisceau partiel. On dira qu'un faisceau partiel est un noyau N si et seulement si :

$$\forall (D_1, D_2) \in K \times (F-K), \text{Card } D_1 \neq \text{Card } D_2.$$

2) - Construction de quasi-groupes mutuellement orthogonaux.

Etant donné un système de Droites (E, F, R) où :

$$F = \{D_1, D_2, \dots, D_b\},$$

supposons l'existence :

- a) d'un noyau $N = \{D_j ; j \in J\}$ où $J \subset \{1, \dots, b\}$
 b) quelque soit $j \in J$ de m quasi-groupes mutuellement orthogonaux $D_j(\phi_j, h)$ $h \in \{1, \dots, m\}$
 c) quel que soit $i \in (\{1, \dots, b\} - J)$ de m quasi-groupes mutuellement orthogonaux idempotents :

$$D_i(\phi_i, h) \quad , h \in \{1, \dots, m\} .$$

Définissons sur E les opérations ψ_h où $h \in \{1, \dots, m\}$ par :

- A) $\forall j \in J$, $\forall (x, y) \in D_j^2$, $x \psi_h y = x \phi_{j,h} y$
 B) $\forall i \in (\{1, \dots, b\} - J)$, $\forall (x, y) \in D_i^2$, $x \neq y$,
 $x \psi_h y = x \phi_{i,h} y$
 C) $\forall x \in E$, $x \notin \{D_j ; j \in J\}$, $x \psi_h x = x$.

Théorème 1.

Les opérations ψ_h où $h \in \{1, \dots, m\}$ définissent sur E , m quasi-groupes mutuellement orthogonaux $E(\psi_h)$.

Démonstration.

- a) $\forall (x, y) \in E^2$, $x \neq y$, il existe une droite unique D_i telle que : $(x, y) \in D_i^2$.
 b) X désignant le sous-ensemble d'indices de $\{1, \dots, b\}$ tel que $t \in X \iff x \in D_t$, la famille de sous-ensemble de points $(D_t - \{x\})$ où $t \in X$, forme une partition de $(E - \{x\})$.

Pour que $E(\psi_h)$ soit un quasi-groupe, il faut et il suffit que :

$$\forall x \in E \quad , \quad \psi_h(x, E) = \psi_h(E, x) = E$$

Soit donc un élément x de E .

1° Cas : $x \cap J \neq \emptyset$.

Soit D_σ la droite de N passant par x .

$$\text{On a : } E = D_\sigma \bigcup_{t \in (X - \{\sigma\})} (D_t - \{x\})$$

Alors :

$$\Psi_h(x, E) = \phi_{\sigma, h}(x, D_\sigma) \bigcup_{t \in (X - \{\sigma\})} \phi_{t, h}[x, (D_t - \{x\})].$$

D'où :

$$\forall t \in (X - \{\sigma\}), \phi_{t, h}[x, (D_t - \{x\})] = D_t - \{x\}$$

et :

$$\Psi_h(x, E) = D_\sigma \bigcup_{t \in (X - \{\sigma\})} (D_t - \{x\}) = E.$$

2° Cas : $x \cap J = \emptyset$.

Alors :

$$E = \{x\} \bigcup_{t \in X} (D_t - \{x\})$$

On a :

$$\Psi_h(x, E) = \{x\} \bigcup_{t \in X} \phi_{t, h}(x, (D_t - \{x\})).$$

d'où :

$$\Psi_h(x, E) = E$$

On montrerait de même : $\forall x \in E, \Psi_h(E, x) = E$.

Pour que deux quasi-groupes $E(\Psi_h)$ et $E(\Psi_k)$ soient orthogonaux, il faut et il suffit que :

$$(S) \quad \begin{cases} x \Psi_k y = z \Psi_k t \\ x \Psi_h y = z \Psi_h t \end{cases}$$

entraîne : $x = z$ et $y = t$.

Soient D_i et D_q les droites contenant respectivement (x, y) et (z, t) .

Le système (S) a un sens si $D_i \cap D_q \neq \emptyset$.

Soit $a = D_i \cap D_q$

Soit par exemple D_q la droite n'appartenant pas à N (il y en a au moins une).

Alors :

$$D_q(\phi_{q,h}) \text{ et } D_q(\phi_{q,k})$$

sont idempotents et :

$$\begin{cases} \mathbb{Z} \phi_{q,h}^t = a \\ \mathbb{Z} \phi_{q,k}^t = a \end{cases}$$

entraîne $\mathbb{Z} = t = a$;

mais alors les opérations $a \phi_{q,h}^a$ et $a \phi_{q,k}^a$ ne correspondent plus aux opérations $a \psi_h^a$ et $a \psi_k^a$.

Donc (S) a un sens si et seulement si x, y, z, t appartiennent à une même droite D_i .

Le système (S) s'écrit alors :

$$\begin{cases} x \phi_{i,h}^y = \mathbb{Z} \phi_{i,h}^t \\ x \phi_{i,k}^y = \mathbb{Z} \phi_{i,k}^t \end{cases}$$

On en déduit : $x = z$ et $y = t$

vu que les quasi-groupes $D_i(\phi_{i,h})$ et $D_i(\phi_{i,k})$ sont orthogonaux.

III. Système de Plans (référence [3])

1) - Définition des Systèmes de plans.

Soient E et F deux ensembles finis d'éléments.

Soit R un sous-ensemble de $E \times F$.

Le triplet (E, F, R) définit un système de plans de dimension k , soit (S_k) , si l'on a les propriétés de définition suivantes :

a) Propriété 1.

Soient h éléments distincts quelconques de F :

$y_{i1}, y_{i2}, \dots, y_{ih}$. On a :

$$(1) \text{ Card } [x; x \in E, (x, y_{i1}) \in R] > \text{ Card } [x; x \in E, (x, y_{i1}) \in R, \\ (x, y_{i2}) \in R] \geq \text{ Card } [x; x \in E, (x, y_{i1}) \in R, (x, y_{i2}) \in R, \\ (x, y_{i3}) \in R] \geq \dots \geq \text{ Card } [x; x \in E, (x, y_{i1}) \in R, \\ (x, y_{i2}) \in R, \dots, (x, y_{ih}) \in R]$$

et ceci pour tout h .

De plus, si dans (1) les signes d'inégalités sont tous stricts, ils le sont encore pour toute permutation de $y_{i1}, y_{i2}, \dots, y_{ih}$, pourvu que :

$$\text{Card } [x; x \in E, (x, y_{i1}) \in R, \dots, (x, y_{ih}) \in R] > 0.$$

Ceci est valable : $\forall h \in [2, k]$.

b) Propriété 2 : Notion d'Indépendance $[2 \leq h \leq k+1]$

h éléments de E : $x_{i1}, x_{i2}, \dots, x_{ih}$ sont indépendants si l'on peut trouver exactement $k-h+1$ éléments distincts de F :

$$y_{j1}, y_{j2}, \dots, y_{jk-h+1}$$

tels que :

$$(x_i, y_j) \in R, \forall i \in [i_1, i_2, \dots, i_h], \forall j \in [j_1, j_2, \dots, j_{k-h+1}]$$

et que :

$$(2) \quad \text{Card} \left[x; x \in E, (x, y_{j_1}) \in R \right] > \text{Card} \left[x; x \in E, (x, y_{j_1}) \in R, \right. \\ \left. (x, y_{j_2}) \in R \right] > \dots > \text{Card} \left[x; x \in E, (x, y_{j_1}) \in R, \right. \\ \left. \dots, (x, y_{j_{k-h+1}}) \in R \right]$$

On dit alors que les éléments $x_{i_1}, x_{i_2}, \dots, x_{i_h}$ de E définissent une variété v à $h-1$ dimensions.

La deuxième propriété est que les inégalités (2) entraînent l'existence de h éléments distincts de E , indépendants : $x_{i_1}, x_{i_2}, \dots, x_{i_h}$ tels que :

$$(x_{i_j}, y_{j_j}) \in R, \quad \forall i \in [i_1, i_2, \dots, i_h], \quad \forall j \in [j_1, j_2, \dots, j_{k-h+1}].$$

Cas particuliers.

$$\alpha) \quad \underline{h = 2}$$

Deux éléments distincts de E sont toujours indépendants.

$$\beta) \quad \underline{h = k}$$

k éléments indépendants de E définissent un élément de F et un seul,

et réciproquement pour tout élément y de F , il existe

k éléments distincts de E , $x_{i_1}, x_{i_2}, \dots, x_{i_k}$ tels que :

$$(x_{i_\alpha}, y) \in R, \quad \forall \alpha \in [1, k]$$

et que $x_{i_1}, x_{i_2}, \dots, x_{i_k}$ soient indépendants.

$$\gamma) \quad \underline{h = k+1}$$

$k+1$ éléments indépendants de E définissent E qui peut être considéré comme une variété à k dimensions.

(Il est alors impossible de trouver un élément y de F

tel que :

$(x_i, y) \in R \quad \forall i \in [1, k+1]$, si $x_1, x_2, \dots, x_{k+1}$ désignent les $k+1$ éléments de E).

c) Propriété 3.

k éléments distincts de E sont incidents à au moins un élément de F :

$$\forall (x_{i_1}, x_{i_2}, \dots, x_{i_k}) \in E^k, x_{i_1} \neq x_{i_2} \neq \dots \neq x_{i_k}$$

$\exists y \in F$, tel que :

$$(x_{i_\alpha}, y) \in R, \quad \forall \alpha \in [1, k].$$

d) Propriété 4.

Soient $h+h'$ éléments de F :

$$y_{i_1} y_{i_2} \dots y_{i_h}, y'_{i_1}, y'_{i_2}, \dots, y'_{i_{h'}}$$

tels que :

$$\text{Card} [x; x \in E, (x, y_{i_1}) \in R] > \dots > \text{Card} [x; x \in E, (x, y_{i_h}) \in R]$$

$$\text{Card} [x; x \in E, (x, y'_{i_1}) \in R] > \dots > \text{Card} [x; x \in E, (x, y'_{i_{h'}}) \in R]$$

Si l'on a :

$$\{x; x \in E, (x, y_{i_1}) \in R, \dots, (x, y_{i_h}) \in R\} =$$

$$\{x; x \in E, (x, y'_{i_1}) \in R, \dots, (x, y'_{i_{h'}}) \in R\}$$

nécessairement :

$$\underline{h = h'}$$

e) Propriété 5.

Soient $x_{i_1}, x_{i_2}, \dots, x_{i_h}$, h éléments distincts de E , indépendants caractérisés par les éléments distincts de F suivants : $y_{j_1}, y_{j_2}, \dots, y_{j_{k-h+1}}$.

Soient d'autre part, $k-h+1$ éléments distincts de F : $y'_{j_1}, y'_{j_2}, y'_{j_3}, \dots, y'_{j_{k-h+1}}$ (dont certains peuvent être différents des $k-h+1$ éléments de F précédents), tels que :

$$\begin{aligned} \text{Card } [x; x \in E, (x, y'_{j_1}) \in R] &> \text{Card } [x; x \in E, (x, y'_{j_1}) \in R, \\ (x, y'_{j_2}) \in R] &> \dots > \text{Card } [x; x \in E, (x, y'_{j_1}) \in R, \dots, \\ & (x, y'_{j_{k-h+1}}) \in R] \end{aligned}$$

et que :

$$(x_{i_1}, y'_{j_1}) \in R, \forall i \in [i_1, i_2, \dots, i_h], \forall j \in [j_1, j_2, \dots, j_{k-h+1}]$$

Alors :

$$\begin{aligned} \{x; x \in E, (x, y_{j_1}) \in R, \dots, (x, y_{j_{k-h+1}}) \in R\} &= \\ \{x; x \in E, (x, y'_{j_1}) \in R, \dots, (x, y'_{j_{k-h+1}}) \in R\} \end{aligned}$$

Ceci est valable pour tout $h \in [2, k-1]$

f) Propriété 6.

Soient h éléments indépendants de E : $x_{i_1}, x_{i_2}, \dots, x_{i_h}$ définissant une variété v de dimension $h-1$, caractérisés par les éléments distincts de F suivants :

$$y_{j_1}, y_{j_2}, \dots, y_{j_{k-h+1}}.$$

Soit d'autre part, un élément quelconque x de E . Les éléments $x_{i_1}, x_{i_2}, \dots, x_{i_h}, x$ de E sont indépendants,

pourvu que les éléments (x, y_{j_1}) , (x, y_{j_2}) , ..., $(x, y_{j_{k-h+1}})$ de $E \times F$ n'appartiennent pas tous à R . Ceci est valable pour tout $h \in [2, k]$.

2) - Propriétés des Systèmes de Plans.

a) Dans toute la suite, les éléments de E seront désignés par des points et les éléments de F seront désignés par des plans. D'autre part, le sous-ensemble R de $E \times F$ va nous permettre d'identifier chaque plan aux points de E avec lesquels, il est en "correspondance".

Soit, en effet, f l'application de F dans $P(E)$, ensemble des parties de E , suivante :

$$f(y) = \{x : x \in E, (x, y) \in R\}$$

Nous allons voir que l'application f ainsi définie est injective.

En effet, supposons par l'absurde que :

$$f(y_1) = f(y_2)$$

et ceci pour deux plans différents y_1 et y_2 de F . En vertu de la propriété 1 de définition des systèmes de plans, on sait que :

$$\text{Card} [x; x \in E, (x, y_1) \in R] > \text{Card} [x; x \in E, (x, y_1) \in R, (x, y_2) \in R]$$

De même :

$$\text{Card} [x; x \in E, (x, y_2) \in R] > \text{Card} [x; x \in E, (x, y_2) \in R, (x, y_1) \in R]$$

Donc :

$$f(y_1) = f(y_2) \implies y_1 = y_2.$$

L'application f est donc bien injective : à chaque plan y correspond une partie différente de E , $f(y)$ qui la caractérise.

On peut donc identifier chaque plan y avec les points qu'il "contient" $f(y)$.

La même remarque va être faite en ce qui concerne les variétés.

Vue la propriété 2 de définition des Systèmes de Plans, une variété v de dimension $h-1$ peut être caractérisée par $k-h+1$ plans : $y_{j1} \ y_{j2} \ \dots \ y_{jk-h+1}$.

En effet, par définition, v est caractérisée par h points indépendants $x_{i1} \ , \ x_{i2} \ , \ \dots \ , \ x_{ih}$, tels que :

$$(x_{i1} \ , \ y_{jn}) \in R \quad , \quad \forall i \in [1, h] \quad , \quad \forall n \in [1, k-h+1]$$

et que :

$$\text{Card} [x; x \in E, (x, y_{j1}) \in R] > \dots > \text{Card} [x; x \in E, (x, y_{j1}) \in R, \dots, (x, y_{jk-h+1}) \in R].$$

On peut remarquer tout de suite que la caractérisation de v par $k-h+1$ plans n'est pas nécessairement unique.

En vertu de la propriété 5 de définition des Systèmes de Plans, il peut se faire qu'il existe $k-h+1$ plans $y'_{j1} \ , \ y'_{j2} \ , \ \dots \ , \ y'_{jk-h+1}$ dont certains sont distincts des précédents et tels que :

$$(x_{i1} \ , \ y'_{jn}) \in R \quad , \quad \forall i \in [1, h] \quad , \quad \forall n \in [1, k-h+1]$$

et :

$$\text{Card} [x; x \in E, (x, y'_{j1}) \in R] > \dots > \text{Card} [x; x \in E, (x, y'_{j1}) \in R, \dots, (x, y'_{jk-h+1}) \in R]$$

Si alors on considère l'application g de l'ensemble des variétés dans $P(E)$ suivante :

$$g(v) = \{ x ; x \in E, (x, y_{j_1}) \in R, \dots, (x, y_{j_{k-h+1}}) \in R \}$$

Il est immédiat de constater que cette application est injective en utilisant les propriétés 4 et 5 de définition des Systèmes de Plans.

En effet, supposons par l'absurde :

$$g(v) = g(v')$$

avec $v \neq v'$.

Supposons que v soit caractérisée par $y_{j_1} y_{j_2} \dots y_{j_{k-h+1}}$ et v' par : $y'_{j_1} y'_{j_2} \dots y'_{j_{k-h+1}}$

La propriété 4 entraîne que $h = h'$ puisque

$$g(v) = g(v') \text{ s'écrit :}$$

$$\begin{aligned} & \{ x ; x \in E, (x, y_{j_1}) \in R, \dots, (x, y_{j_{k-h+1}}) \in R \} = \\ & \{ x ; x \in E, (x, y'_{j_1}) \in R, \dots, (x, y'_{j_{k-h+1}}) \in R \} \end{aligned}$$

Mais alors la propriété 6 entraîne que v et v' peuvent être caractérisées par les mêmes points indépendants de E , par exemple $x_1, x_2, \dots, x_h$.

Autrement dit, $v = v'$.

Et l'application g est donc bien finalement injective. v pourra être identifié à $g(v)$ et la notation $x \in v$ signifiera :

$$(x, y_{j_1}) \in R \text{ et } (x, y_{j_2}) \in R, \dots \text{ et } (x, y_{j_{k-h+1}}) \in R.$$

(Si v est caractérisée par les plans $y_{j_1}, y_{j_2}, \dots, y_{j_{k-h+1}}$).

Ces différentes remarques conduisent à user d'une terminologie analogue à celle des réseaux géométriques au chapitre I, c'est-à-dire de parler d'intersections de plans et de les noter $y_{j_1} \cap y_{j_2} \cap \dots \cap y_{j_h}$, du nombre

de points d'un plan ou d'une variété et de les noter :

$$\text{Card} [y_{j1} \cap y_{j2} \cap \dots \cap y_{jh}],$$

une variété n'étant que l'ensemble des points communs aux plans qui la caractérise.

Insistons enfin sur le fait que les propriétés 4 et 5 de définition des Systèmes de Plans étaient nécessaires pour justifier la caractérisation des variétés. Ainsi, soit la variété $v = y_1 \cap y_2$, intersection des plans y_1 et y_2 .

Soit, d'autre part, y un plan contenant la variété v et différent de y_1 et y_2 .

Dans ces conditions, $y \cap y_1$ caractérise une variété qui doit être identique à v , ce qui est le cas en vertu de la propriété 5. (Sinon la définition d'une variété donnée à la propriété 2 serait mauvaise, des points indépendants pouvant définir plusieurs variétés).

De la même façon, la propriété 4 est nécessaire pour qu'un ensemble de points soit défini par le même nombre de points indépendants.

b) La propriété 6 signifie que, étant donnée une variété v de dimension $h-1$ caractérisée par h de ses points $x_{i1}, x_{i2}, \dots, x_{ih}$ indépendants, $\forall x \in E, x \notin v$, les points $x_{i1}, x_{i2}, \dots, x_{ih}$ et x sont indépendants et caractérisent une variété de dimension h contenant la variété v .

Nous avons défini l'indépendance de h points. Il s'agirait de s'inquiéter maintenant du cas contraire où h points ne sont pas indépendants.

Soient donc h points quelconques non indépendants $x_1, x_2, \dots, x_h$. ($h > 2$).

On sait que deux d'entre eux quelconques x_1 et x_2 , par exemple, sont toujours indépendants (propriété 2 de définition des Systèmes de Plans). Donc il existe exactement $k-1$ plans $y_1 y_2 \dots y_{k-1}$ tels que :

$$(x_i, y_j) \in R, \quad \forall i \in [1, 2], \quad \forall j \in [1, k-1].$$

x_1 et x_2 définissent une variété v_1 à une dimension.

Considérons alors les autres points x_i , $i \in [3, h]$.

(1) Si $(x_i, y_j) \in R$, $\forall i \in [3, h]$, $\forall j \in [1, k-1]$, on a donc

$$x_i \in v_1, \quad \forall i > 2$$

et les points x_i $\forall i > 2$ "dépendent" de x_1 et x_2 .

(2) Si $x_3 \notin y_1 \cap y_2 \cap \dots \cap y_{k-1} = v_1$, c'est-à-dire

si $(x_3, y_j) \in R$ n'est pas vérifié pour tout $j \in [1, k-1]$, on sait par application de la propriété 6 de définition des Systèmes de Plans que x_1 x_2 et x_3 sont indépendants.

Il existe alors $k-2$ plans $y'_1 y'_2 \dots y'_{k-2}$ avec les propriétés de la propriété 2 de définition des Systèmes de Plans. On peut recommencer le même procédé.

.....

Finalement, on extrait des points $x_1 x_2 \dots x_h$, h_1 points indépendants, par exemple $x_1 x_2 \dots x_{h_1}$. Ces h_1 points définissent une variété v_{h_1-1} à h_1-1 dimensions, contenant les autres points x_i : $x_i \in v_{h_1-1}$, $\forall i \in [h_1+1, h]$.

Ceci peut encore être exprimé de la façon suivante :
Si h est le nombre maximum de points indépendants extraits d'un sous-ensemble S de E , ces h points définissent une variété à $h-1$ dimensions contenant tous les points de S .

c) Si $x_{i_1}, x_{i_2}, \dots, x_{i_h}$ sont h points distincts de E indépendants, les points $x_{i_1}, x_{i_2}, \dots, x_{i_{h-1}}$ sont également indépendants.

Ceci est facilement vérifiable.

Si on suppose en raisonnant, par l'absurde, que les points $x_{i_1}, x_{i_2}, \dots, x_{i_{h-1}}$ ne sont pas indépendants, soit v la variété qu'ils définissent, variété dont la dimension sera inférieure à $h-2$, dès lors $x_{i_1} x_{i_2} \dots x_{i_h}$ ne pourront plus définir une variété de dimension $h-1$ de par la propriété b) précédente. Les points $x_{i_1} x_{i_2} \dots x_{i_{h-1}}$ sont donc indépendants.

Plus généralement, étant donné h points indépendants $x_1, x_2, \dots, x_h$, ceci entraîne que les points $x_{i_1}, x_{i_2}, \dots, x_{i_h}$ le sont également :

$$\forall h_1 < h \quad \forall (i_1 i_2 \dots i_{h_1}) \subset (1, 2, \dots, h), \\ i_1 \neq i_2 \neq \dots \neq i_{h_1}.$$

d) L'intersection d'un Système de Plans (S_k) par un plan y de ce système est un système de plans (S_{k-1}) : les points de ce système sont les points de y et les plans les intersections des plans de S_k avec y .

Cette propriété découle immédiatement des propriétés précédentes.

e) Soit v_h une variété de dimension h . Soit $\{v_h\}$ l'ensemble des points de v_h . On a :

$$E = \{v_h\} \cup \left[\bigcup_{\forall v_{h+1} \supset v_h} \{v_{h+1} - v_h\} \right]$$

Le recouvrement de E ainsi obtenu est une partition de E .

($\{v_{h+1} - v_h\}$ représente l'ensemble des points de la variété v_{h+1} auquel on a oté les points de v_h).

Cette propriété est également aisément vérifiable. Soit x un point n'appartenant pas à v_h . x et v_h définissent une variété v_{h+1}^x contenant v_h .

Soit y un point n'appartenant pas à v_{h+1}^x . y et v_h définissent une variété v_{h+1}^y contenant v_h .

D'où le recouvrement de E annoncé.

Il reste à montrer que c'est une partition, c'est-à-dire que :

$$\{v_{h+1}^x - v_h\} \cap \{v_{h+1}^y - v_h\} = \emptyset$$

S'il n'en était pas ainsi et que v_{h+1}^x et v_{h+1}^y aient en commun un point z de E n'appartenant pas à v_h , les deux variétés auraient en commun une variété de dimension $h+1$; elles seraient donc confondues, ce qui est contraire à l'hypothèse.

f) Définition.

Un sous-ensemble F_1 de F sera un noyau si l'on a :

$$\forall (y_1, y_2) \in F_1^2, \quad y_1 \neq y_2 :$$

$$\text{Card} [x ; x \in E, (x, y_1) \in R, (x, y_2) \in R] = 0$$

Les plans d'un noyau n'ayant pas de points communs sont dits parallèles.

3) - Définition de la propriété (P).

Soit v une variété de dimension $h-1$ d'un système de plans (S_k) .

Considérons v comme un ensemble de points (ou d'éléments) et soit alors un arrangement (T_k) sur v :

$$[x_1, x_2, \dots, x_k ; f(x_1, x_2, \dots, x_k)] , \forall (x_1, x_2, \dots, x_k) \in v^k$$

On dira que cet arrangement (T_k) possède la propriété (P), si et seulement si, pour tout sous-ensemble S de k points de v : $x_1, x_2, \dots, x_k$, le point de v suivant :

$$x = f(x_1, x_2, \dots, x_k)$$

est indépendant de tout sous-ensemble de $h-1$ points extraits de S . (Les k points de S ne sont pas nécessairement distincts)

4) - Construction d'un arrangement (T_k) sur E .

- Dans tout ce paragraphe 4), ainsi que dans tout le paragraphe 5) suivant, quand nous définirons un arrangement (T) sur un plan y ou de façon plus générale, un arrangement (T_k) sur une variété v , cela voudra dire que nous considérons y ou v comme des ensembles d'éléments, les éléments de y ou v étant identifiés aux points de y ou v .

- De même, nous avons vu que toute variété v d'un système de plans pouvait être définie comme étant l'intersection d'un certain nombre de plans et ceci au moins d'une façon. Dans toute la suite (paragraphe 5) compris), quand nous parlerons d'une variété v , intersection des plans $y_1, y_2, \dots, y_h$, nous entendrons par là tous les plans passant par v (Il est bien certain que l'on n'a pas forcément besoin de tous les plans passant par v pour caractériser v , mais cette précaution nous évitera des ambiguïtés de langage qui subsisteraient sans cette précaution).

- Soit un système de plans $(S_k) = (E, F, R)$

avec $F = \{y_1, y_2, \dots, y_N\}$.

Supposons l'existence d'un noyau K :

$$K = \left\{ y_i ; i \in J \subset [1, N] \right\}.$$

Soient :

a) $\forall i \in J$, un arrangement (T_k) sur le plan y_i :

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)] , (x_1, x_2, \dots, x_k) \in y_i^k$$

b) $\forall i \in \bigcup_{[1, N]} J$, un arrangement (T_k) sur y_i , idempotent

et possédant la propriété (P) :

$$[x_1, x_2, \dots, x_k ; f_i(x_1, x_2, \dots, x_k)] , (x_1, x_2, \dots, x_k) \in y_i^k$$

c) Pour toute variété v intersection de plans : $y_{i_1}, y_{i_2}, \dots, y_{i_h}$ n'appartenant pas au noyau K , un arrangement (T_k) sur v , idempotent et possédant la propriété (P) :

$$[x_1, x_2, \dots, x_k ; f_{i_1 i_2 \dots i_h}(x_1, x_2, \dots, x_k)] , \\ (x_1, \dots, x_k) \in v^k$$

Théorème 1.

Les données précédentes permettent de définir un arrangement (T_k) sur E :

$$[x_1, x_2, \dots, x_k ; F(x_1, x_2, \dots, x_k)] , (x_1, \dots, x_k) \in E^k$$

de la façon suivante :

$$\text{Soit : } (x_1, x_2, \dots, x_k) \in E^k,$$

(1) Si les points $(x_1, x_2, \dots, x_k)$ appartiennent à un

plan y_i du noyau K , alors :

$$F(x_1, x_2, \dots, x_k) = f_i(x_1, x_2, \dots, x_k) \\ (\forall i \in J)$$

(2) Si les points $(x_1, x_2, \dots, x_k)$ définissent un plan y_i n'appartenant pas au noyau K , alors :

$$F(x_1, x_2, \dots, x_k) = f_i(x_1, x_2, \dots, x_k). \\ (\forall i \in \bigcup_{[1, N]} J)$$

(3) Si les points $(x_1, x_2, \dots, x_k)$ définissent une variété v intersection des plans $y_{i_1}, y_{i_2}, \dots, y_{i_h}$ aucun des plans y_{i_e} ne pouvant appartenir au noyau K , alors :

$$F(x_1, x_2, \dots, x_k) = f_{i_1 i_2 \dots i_h}(x_1, x_2, \dots, x_k).$$

Démonstration.

Il s'agit de montrer que :

$$(\forall i), (\forall (x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_k) \in E^{k-1}),$$

$$F(x_1, x_2, \dots, x_{i-1}, E, x_{i+1}, \dots, x_k) = E.$$

Il suffit, bien sûr, de montrer par exemple que :

$$\forall (x_1, x_2, \dots, x_{k-1}) \in E^{k-1} : F(x_1, x_2, \dots, x_{k-1}, E) = E$$

1° Cas.

Les points $x_1, x_2, \dots, x_{k-1}$ sont dans un plan y_i du noyau K et y définissent une variété v_h (de dimension h).

On a montré à propos des propriétés des systèmes

de plans que l'on avait :

$$E = \{v_h\} \cup \left[\bigcup_{\substack{\forall v_{h+1} \supset v_h \\ v_{h+1} \in y_i}} \{v_{h+1} - v_h\} \right] \cup \left[\bigcup_{\substack{\forall v_{h+1} \supset v_h \\ v_{h+1} \notin y_i}} \{v_{h+1} - v_h\} \right]$$

(v_{h+1} désignant une variété de dimension $h+1$).

Soit d'autre part :

$$\Psi(E) = F(x_1, x_2, \dots, x_{k-1}, E).$$

On a :

$$\{y_i\} = \{v_h\} \cup \left[\bigcup_{\substack{\forall v_{h+1} \supset v_h \\ v_{h+1} \in y_i}} \{v_{h+1} - v_h\} \right]$$

Or sur y_i est défini un arrangement (T_k) :

$$[x_1, x_2, \dots, x_k; f_i(x_1, x_2, \dots, x_k)] \quad \text{et on a :}$$

$$F(x_1, x_2, \dots, x_k) = f_i(x_1, x_2, \dots, x_k)$$

$$\forall (x_1, x_2, \dots, x_k) \in y_i^k.$$

$$\text{Donc : } \Psi(\{y_i\}) = \{y_i\}.$$

Seul reste à considérer :

$$\Psi \left[\bigcup_{\substack{\forall v_{h+1} \supset v_h \\ v_{h+1} \notin y_i}} \{v_{h+1} - v_h\} \right]$$

expression qui est égale à :

$$\bigcup_{\substack{v_{h+1} \supset v_h \\ v_{h+1} \not\subset y_i}} \Psi(\{v_{h+1} - v_h\})$$

- Chaque variété v_{h+1} est l'intersection d'un certain nombre de plans $y_{i_1} y_{i_2} \dots y_{i_l}$. Sur chaque variété v_{h+1} est donc définie une structure d'arrangement (T_k) :

$$\left[x_1, x_2, \dots, x_k ; f_{i_1 i_2 \dots i_l} (x_1, x_2, \dots, x_k) \right],$$

$$(x_1, \dots, x_k) \in v_{h+1}^k$$

Les variétés v_{h+1} considérées ici coupent y_{i_1} plan du noyau sans y appartenir. Les variétés v_{h+1} ne peuvent donc appartenir à un autre plan du noyau. L'arrangement (T_k) précédent est donc idempotent et il possède la propriété (P). Donc :

$$\bigcup_{\substack{v_{h+1} \supset v_h \\ v_{h+1} \not\subset y_i}} \Psi(\{v_{h+1} - v_h\}) = \bigcup_{\substack{v_{h+1} \supset v_h \\ v_{h+1} \not\subset y_i}} \{v_{h+1} - v_h\}$$

On est certain en effet de par la propriété (P) de ne pas obtenir v_h (on a une variété à $h+1$ dimensions v_{h+1} , dans cette variété k points $x_1, x_2, \dots, x_{k-1}$ et x . Parmi les points $x_1, x_2, \dots, x_{k-1}$, il y en a $h+1$ $x_{i_1}, x_{i_2}, \dots, x_{i_{h+1}}$ qui sont indépendants et qui définissent v_h :

$x_{i_1}, x_{i_2}, \dots, x_{i_{h+1}}$ et x caractérisent alors v_{h+1} .

On sait enfin que le point :

$$\Psi(x) = f_{i_1 i_2 \dots i_l}(x_1, x_2, \dots, x_{k-1}, x)$$

n'appartiendra pas à v_h , de par la propriété (P)).

Finalement donc :

$$\Psi(E) = E.$$

2° Cas.

Les points $x_1, x_2, \dots, x_{k-1}$ ne sont pas dans un plan

y_i du noyau K et ils définissent une variété v_h (à h dimensions).

C'est exactement le même type de démonstration, excepté que les plans du noyau ne jouent évidemment plus aucun rôle.

On a :

$$E = \{v_h\} \cup \left[\bigcup_{\forall v_{h+1} \supset v_h} \{v_{h+1} - v_h\} \right]$$

(la notation v_{h+1} désignant une variété à $h+1$ dimensions).

Supposons que la variété v_h soit à l'intersection de h plans $y_{i_1}, y_{i_2}, \dots, y_{i_h}$. Est défini alors sur v_h un arrangement (T_k) :

$$[x_1, x_2, \dots, x_k ; f_{i_1} i_2 \dots i_h(x_1, x_2, \dots, x_k)]$$

et cet arrangement est idempotent et possède la propriété (P) puisqu'aucun des plans y_{i_j} ne peut appartenir au noyau K par hypothèse.

En posant toujours :

$$\Psi(E) = F(x_1, x_2, \dots, x_{k-1}, E)$$

On a :

$$\Psi(\{v_h\}) = \{v_h\}.$$

De même, pour chaque variété v_{h+1} contenant v_h :

$$\Psi(\{v_{h+1} - v_h\}) = \{v_{h+1} - v_h\} ,$$

puisque l'arrangement (T_k) que l'on définit sur chaque v_{h+1} possède la propriété (P).

On a donc encore une fois :

$$\Psi(E) = E.$$

Remarque.

L'idempotence est requise dans certains cas particuliers, ceux où $x_1, x_2, \dots, x_{k-1}$ sont égaux à un seul point. Dans ces conditions, la propriété (P) se confond avec l'idempotence, que l'on pourrait se dispenser de signaler dans les énoncés. Si cela n'a pas été fait, c'est que la propriété (P) est bien particulière dans ces cas.

5) - Construction d'arrangements (T_k) orthogonaux sur E.

- Soit un système de plans $(S_k) = (E, F, R)$
- avec : $F = \{y_1, y_2, \dots, y_N\}$.
- Supposons l'existence d'un noyau K :

$$K = \left\{ y_j ; y_j \in F, \quad j \in J \subset [1, N] \right\}.$$

Soient :

- a) $\forall i \in J$, h arrangements (T_k) orthogonaux sur le plan y_i :

$$[x_1, x_2, \dots, x_k ; f_i^1(x_1, x_2, \dots, x_k)] , (x_1, x_2, \dots, x_k) \in y_i^k ,$$

$$1 \in [1, h] .$$

b) $\forall i \in \bigcup_{[1, N]} J$, h arrangements (T_k) orthogonaux sur le plan y_i :

$$\left[x_1, x_2, \dots, x_k ; f_i^1(x_1, x_2, \dots, x_k) \right], (x_1, x_2, \dots, x_k) \in y_i^k, \\ 1 \in [1, h].$$

Ces arrangements étant d'autre part idempotents et possédant chacun la propriété (P).

c) Pour toute variété v intersection des plans $y_{i_1}, y_{i_2}, \dots, y_{i_{h_1}}$ n'appartenant pas au noyau K , h arrangements (T_k) orthogonaux :

$$\left[x_1, x_2, \dots, x_k ; f_{i_1}^1 \dots f_{i_{h_1}}^1(x_1, \dots, x_k) \right], \\ (x_1, \dots, x_k) \in v^k, \quad 1 \in [1, h].$$

Ces arrangements étant d'autre part idempotents et possédant chacun la propriété (P).

Théorème 2.

Les données précédentes permettent de définir sur E h arrangements (T_k) orthogonaux :

$$\left[x_1, x_2, \dots, x_k ; F_1(x_1, x_2, \dots, x_k) \right], (x_1, \dots, x_k) \in E^k, \\ 1 \in [1, h],$$

de la façon suivante :

Soit $(x_1, x_2, \dots, x_k) \in E^k$.

(1) Si $(x_1, x_2, \dots, x_k)$ définissent un plan y_i n'appartenant pas au noyau K , alors :

$$F_1(x_1, x_2, \dots, x_k) = f_i^1(x_1, x_2, \dots, x_k), \quad \forall 1 \in [1, h].$$

(2) Si $(x_1, x_2, \dots, x_k)$ appartiennent à un plan y_i du noyau K , alors :

$$F_1(x_1, x_2, \dots, x_k) = f_i^1(x_1, x_2, \dots, x_k) \quad , \quad \forall i \in [1, h] .$$

(3) Si $(x_1, x_2, \dots, x_k)$ définissent une variété v intersection des plans $y_{i_1} y_{i_2} \dots y_{i_h}$, aucun des plans y_{i_1} n'appartenant au noyau K , alors :

$$F_1(x_1, x_2, \dots, x_k) = f_{i_1 i_2 \dots i_h}^1(x_1, x_2, \dots, x_k) \quad , \quad \forall i \in [1, h] .$$

Démonstration.

Démontrons par exemple que le système suivant de h_1 équations à h_1 inconnues $X_1, X_2, \dots, X_{h_1}$ a une solution et une seule :

$$\begin{cases} F_1(X_1, X_2, \dots, X_{h_1}, x_{h_1+1}, \dots, x_k) = a_1 \\ 1 = 1, 2, \dots, h. \end{cases}$$

Raisonnons par l'absurde et supposons que le système proposé admette deux solutions distinctes $(X_1, X_2, \dots, X_{h_1})$ et $(X'_1, X'_2, \dots, X'_{h_1})$.

On aurait donc :

$$(S) \quad \begin{cases} F_1(X_1, X_2, \dots, X_{h_1}, x_{h_1+1}, \dots, x_k) = \\ F_1(X'_1, X'_2, \dots, X'_{h_1}, x_{h_1+1}, \dots, x_k) \\ 1 \in [1, h] . \end{cases}$$

Soit v la variété définie par les points :

$X_1, X_2, \dots, X_{h_1}, x_{h_1+1}, \dots, x_k$. Soit v' la variété définie

par les points : $X'_1, X'_2, \dots, X'_{h_1}, x_{h_1+1}, \dots, x_k$.

Le système (S) ne peut avoir un sens que si $a_1 \in \{v\} \cap \{v'\}$ donc si $\{v\} \cap \{v'\} \neq \emptyset$ (ce qui est le cas présent).

Dès lors, deux cas sont possibles.

1° Cas.

Les variétés v et v' sont dans un même plan y_i du noyau K .

On peut alors écrire :

$$\begin{cases} f_i^1(x_1, x_2, \dots, x_{h_i}, x_{h_i+1}, \dots, x_k) = \\ f_i^1(x'_1, x'_2, \dots, x'_{h_i}, x'_{h_i+1}, \dots, x_k) = a_1 \\ \forall i \in [1, h] . \end{cases}$$

Ce qui est impossible puisque les arrangements (T_k) correspondants sur y_i sont orthogonaux.

2° Cas.

Les deux variétés v et v' ne sont pas dans un même plan du noyau K .

Supposons par exemple que v' ne soit pas dans un plan du noyau.

On a alors, si la variété v' est l'intersection des plans $y_{i1}, y_{i2}, \dots, y_{ih_2}$:

$$\begin{cases} f_{i1 \ i2 \ \dots \ ih_2}^1(x'_1, x'_2, \dots, x'_{h_i}, x'_{h_i+1}, \dots, x_k) = a_1 \\ \forall i \in [1, h] . \end{cases}$$

D'autre part, les points $a_1, a_2, \dots, a_h$ doivent appartenir à $v \cap v'$. Ils définissent donc une variété incluse

dans v' . La propriété (P) que possèdent par hypothèse les arrangements (T_k) ci-dessus est par conséquent mise en défaut à moins que les variétés v et v' ne soient confondues. Alors :

$$x_1, x_2, \dots, x_{h_1}, x'_{1_1}, x'_{2_2}, \dots, x'_{h_1}, x_{h_1+1}, \dots, x_k$$

appartiennent à une même variété v , avec par exemple :

$$v = y_{i_1} \cap y_{i_2} \cap \dots \cap y_{i_{h_2}}.$$

Sur cette variété sont définis par hypothèse des arrangements (T_k) orthogonaux. On aurait donc :

$$\left\{ \begin{array}{l} f_{i_1 i_2 \dots i_{h_2}}^{1_1}(x_1, x_2, \dots, x_{h_1}, x_{h_1+1}, \dots, x_k) = \\ f_{i_1 i_2 \dots i_{h_2}}^{1_2}(x'_{1_1}, x'_{2_2}, \dots, x'_{h_1}, x_{h_1+1}, \dots, x_k) \\ \forall i \in [1, h] \end{array} \right.$$

ce qui est impossible, à moins que :

$$\left\{ \begin{array}{l} x_1 = x'_{1_1} \\ x_2 = x'_{2_2} \\ \dots \\ x_{h_1} = x'_{h_1} \end{array} \right.$$

c. q. f. d.

IV. Réseaux associés à l'étude des réseaux (R).

A) - Les réseaux (R)'.

1) - Définition des réseaux (R)'.

Soit E un ensemble fini d'éléments désignés par des points.
Soit F un ensemble fini d'éléments désignés par des plans.

Soit R un sous-ensemble de $E \times F$.

Supposons l'existence d'un plan y_0 de F , tel que la relation S suivante entre plans de $F - \{y_0\}$:

$$\forall (y_i, y_j) \in [F - \{y_0\}]^2, y_i S y_j \iff y_i = y_j$$

ou bien :

$$(x, y_i) \in R \text{ et } (x, y_j) \in R \implies (x, y_0) \in R,$$

soit une relation d'équivalence.

Désignons par $F_1, F_2, \dots, F_N$ les classes d'équivalence de cette relation S .

Soient k et q deux nombres entiers positifs ($k < N$).
Si l'on a :

$$a) \forall x \in E \text{ tel que } (x, y_0) \notin R, \forall i \in [1, N] :$$

$$\text{Card} [y : y \in F_i, (x, y) \in R] = 1$$

$$b) \forall (y_1, y_2) \in F^2, y_1 \neq y_2 :$$

$$\text{Card} [x : (x, y_1) \in R, (x, y_2) \in R] = \frac{q^{k-1} - 1}{q - 1}$$

$$c) \forall (y_1, y_2, \dots, y_h) \in F^h, y_1 \neq y_2 \neq \dots \neq y_h :$$

$$\text{Card} [x : (x, y_1) \in R, (x, y_2) \in R, \dots, (x, y_h) \in R] =$$

$$\alpha) \text{ soit } \frac{q^{k-1} - 1}{q - 1}, \text{ soit } \frac{q^{k-2} - 1}{q - 1}, \dots, \text{ soit } \frac{q^{k-h+1} - 1}{q - 1}$$

si $2 < h \leq k$

$$\beta) \text{ soit } \frac{q^{k-1} - 1}{q - 1}, \text{ soit } \frac{q^{k-2} - 1}{q - 1}, \dots, \text{ soit } 1, \text{ soit } 0$$

si $h > k$.

$$d) \quad \forall h, 2 \leq h \leq k, \quad \exists (i_1, i_2, \dots, i_h) \in [1, N]^h, \\ i_1 \neq i_2 \neq \dots \neq i_h \quad \text{tels que :}$$

$$\forall (y^1, y^2, \dots, y^h) \in F_{i_1} \times F_{i_2} \times \dots \times F_{i_h} :$$

$$\text{Card} [x : x \in E, (x, y^1) \in R, (x, y^2) \in R, \dots, (x, y^h) \in R] = \\ \frac{q^{k-h+1} - 1}{q - 1}$$

$$e) \quad \forall (y_1, y_2) \in F^2, y_1 \neq y_2 :$$

$$\text{Card} [x : (x, y_1) \in R, x \in E] > \text{Card} [x : x \in E, (x, y_1) \in R, (x, y_2) \in R]$$

- Le système (E, F, R, y_0, N, q, k) définit alors un réseau $(R)'$ de dimension k .

2) - Propriétés des réseaux $(R)'$.

a) Considérons l'application f de F dans $P(E)$, ensemble des parties de E , suivante :

$$\forall y \in F : f(y) = \{x : x \in E, (x, y) \in R\}.$$

L'application ainsi définie est injective.

En effet, supposons par l'absurde que $f(y_1) = f(y_2)$, $(y_1, y_2) \in F^2, y_1 \neq y_2$.

On aurait alors :

$$\text{Card} [x : x \in E, (x, y_1) \in R] = \text{Card} [x : x \in E, (x, y_2) \in R] = \\ \text{Card} [x : x \in E, (x, y_1) \in R, (x, y_2) \in R].$$

Cela est impossible, vue la propriété e) de définition des réseaux $(R)'$.

On a donc bien :

$$f(y_1) \neq f(y_2)$$

pour $y_1 \neq y_2$.

Dans ces conditions, on peut confondre $y \in F$ avec $f(y) \in P(E)$ et un plan de F est donc confondu avec la partie de E correspondante.

C'est ce que nous ferons dans toute la suite, où nous emploierons finalement la même terminologie qu'au chapitre I à propos des réseaux (R) et qu'à ce même chapitre V à propos des systèmes de plans.

Ainsi on notera :

$$y_1 \cap y_2$$

pour :

$$\{x : x \in E, (x, y_1) \in R, (x, y_2) \in R\},$$

on parlera de points appartenant à un plan y_1 , appartenant à l'intersection des plans y_1 et y_2 , etc ...

b) On peut remarquer que les plans d'une même classe se coupent suivant $\frac{q^{k-1}-1}{q-1}$ points du plan y_0 .

En effet, soient :

$$y_i \text{ S } y_j$$

avec :

$$(y_i, y_j) \in F \alpha^2, \quad y_i \neq y_j.$$

En appliquant la propriété b) de définition des réseaux (R) , on a :

$$\text{Card } [y_0 \cap y_i] = \text{Card } [y_0 \cap y_j] = \text{Card } [y_i \cap y_j] = \frac{q^{k-1}-1}{q-1}$$

D'autre part :

$$y_i \cap y_j \subset y_0.$$

Donc :

$$\text{Card } [y_0 \cap y_i \cap y_j] = \frac{q^{k-1}-1}{q-1}$$

Finalement :

$$\underline{y_0 \cap y_i = y_0 \cap y_i \cap y_j}$$

Cette égalité est valable $\forall y_j \in F_\infty$; on a donc bien le résultat annoncé, à savoir que les plans d'une même classe se coupent suivant $\frac{q^{k-1}-1}{q-1}$ points du plan y_0 .

c) Soient y_i et y_j deux plans de deux classes différentes F_i et F_j . On a :

$$\text{Card } [y_i \cap y_j \cap y_0] = \frac{q^{k-2}-1}{q-1}$$

(Effectivement, on ne peut avoir $\frac{q^{k-1}-1}{q-1}$ puisque l'on a deux plans de deux classes différentes et vue la propriété c) de définition des réseaux (R) : il n'y a plus que $\frac{q^{k-2}-1}{q-1}$ comme possibilité).

Le nombre de points de $y_i \cap y_j$ n'appartenant pas à y_0 est donc égal à :

$$\frac{q^{k-1}-1}{q-1} - \frac{q^{k-2}-1}{q-1} = q^{k-2}$$

Soit alors q_i le nombre de plans de la classe F_i et soit n_j le nombre de points de y_j .

On a :

$$n_j = q_i q^{k-2} + \frac{q^{k-1}-1}{q-1}$$

[puisque par tout point de $E - \{y_0\}$; il passe un plan et un seul de chaque classe (propriété a) de définition des réseaux (R) :)].

Si l'on répète ce décompte de points pour une autre classe de plans F_1 , on obtient en usant des mêmes notations :

$$n_j = q_1 q^{k-2} + \frac{q^{k-1} - 1}{q - 1}$$

D'où en égalisant et en simplifiant :

$$\underline{q_i = q_1}$$

soit :

Chaque classe contient le même nombre de plans.

d) Appliquons maintenant la propriété d) de définition des réseaux (R)'.

Soient F_1, F_2, F_3 trois classes de plans telles que :

$$\forall (y_1, y_2, y_3) \in F_1 \times F_2 \times F_3$$

l'on ait :

$$\text{Card} [y_1 \cap y_2 \cap y_3] = \frac{q^{k-2} - 1}{q - 1}$$

Montrons tout d'abord que l'on a :

$$\text{Card} [y_1 \cap y_2 \cap y_3 \cap y_0] = \frac{q^{k-3} - 1}{q - 1}$$

Effectivement, supposons par l'absurde que :

$$\text{Card} [y_1 \cap y_2 \cap y_3 \cap y_0] = \frac{q^{k-2} - 1}{q - 1}$$

Ceci entraîne que y_3 passe par $y_1 \cap y_2 \cap y_0$ puisque l'on sait que :

$$\text{Card} [y_1 \cap y_2 \cap y_0] = \frac{q^{k-2} - 1}{q - 1}$$

Soit alors x un point quelconque de $y_1 \cap y_2$ n'appartenant pas à y_0 et soit y'_3 le plan de la classe F_3 passant par x .

y'_3 (comme y_3) passe par $y_1 \cap y_2 \cap y_0$ (puisque $y'_3 \subset y_3$).

Autrement dit :

$$\text{Card} [y_1 \cap y_2 \cap y'_3] > \frac{q^{k-2} - 1}{q - 1}$$

(puisque y'_3 passe aussi par x).

Donc :

$$\text{Card} [y_1 \cap y_2 \cap y'_3] = \frac{q^{k-1} - 1}{q - 1}$$

ce qui est impossible par hypothèse.

On aboutit donc à une contradiction et finalement :

$$\text{Card} [y_1 \cap y_2 \cap y_3 \cap y_0] = \frac{q^{k-3} - 1}{q - 1}$$

De ce premier résultat, on peut déduire le nombre de points de $y_1 \cap y_2 \cap y_3$ n'appartenant pas à y_0 ; soit :

$$\frac{q^{k-2} - 1}{q - 1} - \frac{q^{k-3} - 1}{q - 1} = q^{k-3}$$

En faisant alors varier y_3 dans F_3 , on obtient si n désigne le nombre de plans de F_3 :

$$q^{k-3} n = q^{k-2}$$

$$\text{D'où : } \underline{n = q}$$

Chaque classe de plans contient q plans.

On vérifie aisément que :

Chaque plan de chaque classe contient $\frac{q^k - 1}{q - 1}$ points.

e) Soient $y_1, y_2, \dots, y_h$, h plans d'un réseau (R) de h classes différentes, tels que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = \frac{q^{k-i+1} - 1}{q - 1}$$

$$(i \leq h)$$

Il est alors possible d'extraire i plans :

$y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_i}$ des h plans précédents tels que :

$$y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_i} = y_1 \cap y_2 \cap \dots \cap y_h$$

Démonstration.

Cette propriété se démontre par récurrence. Le raisonnement est en tout point analogue à celui effectué dans la démonstration de la propriété 5 dans le chapitre I.

En effet, on peut remarquer que la propriété est vérifiée pour $i = 2$.

Supposons alors la propriété exacte jusqu'au rang $i-1$. Soient alors les h plans $y_1, y_2, \dots, y_h$ tels que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = \frac{q^{k-i+1} - 1}{q - 1} \quad (i \leq h)$$

- Supposons d'abord que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = \frac{q^{k-i+j+1} - 1}{q - 1}$$

avec $j > 1$.

On peut, en vertu de l'hypothèse de récurrence, extraire $i-j$ plans $y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{i-j}}$ des plans $y_1, y_2, \dots, y_{h-1}$ tels que :

$$\text{Card} [y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-j}}] = \frac{q^{k-i+j+1} - 1}{q - 1}$$

et plus précisément que :

$$y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-j}} = y_1 \cap y_2 \cap \dots \cap y_{h-1}$$

Mais alors la propriété c) de définition des réseaux $(R)'$ est mise en défaut si $j > 1$ puisque

$$\text{Card} [y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-j}} \cap y_h]$$

doit être égal à $\frac{q^{k-i+1}-1}{q-1}$ (et qu'il ne peut ici être égal qu'à $\frac{q^{k-i+j+1}-1}{q-1}$ ou $\frac{q^{k-i+j}-1}{q-1}$).

La seule possibilité est donc que j soit égal à 1, c'est-à-dire que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = \frac{q^{k-i+2}-1}{q-1}$$

$y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{i-j}}$ et y_h constituent alors la famille de plans cherchée, c'est-à-dire telle que :

$$y_1 \cap y_2 \cap \dots \cap y_h = y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{i-1}} \cap y_h$$

-Si l'on suppose maintenant que :

$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = \frac{q^{k-i+1}-1}{q-1}$, on peut alors éliminer le plan y_h et recommencer le même raisonnement pour les plans $y_1, y_2, \dots, y_{h-1}$ restants.

D'où la propriété énoncée.

c. q. f. d.

f) Il reste à étudier le plan y_0 . Si l'on admet qu'il peut y exister des points par lesquels il ne passe pas de plans, on prendra par analogie :

$$\begin{aligned} \text{Card} [y_0] &= \frac{q^{k-1}-1}{q-1} \quad \text{et on aura :} \\ \text{Card} [E] &= \frac{q^{k+1}-1}{q-1} \end{aligned}$$

Sinon, on ne pourrait compter les points de y_0 sans préciser davantage la structure combinatoire du réseau $(R)'$.

g) On peut enfin observer que si l'on retire le plan y_0 du réseau $(R)'$ précédent à k dimensions, on obtient un réseau (R) à k dimensions :

$$\{E', F', R', F_i, i \in [1, N], q, k\}$$

E' représentant l'ensemble des points de E dont on a retiré les points de y_0 , F' l'ensemble des plans de F dont on a retiré y_0 , R' désignant le sous-ensemble de $E' \times F'$ que l'on déduit directement de R .

Démonstration.

Les propriétés a) et b) de définition des réseaux (R) sont aisément vérifiables. Seules restent à être justifiées les propriétés c) et d).

$\proptoPropriété c).$

Soient h plans $y_1, y_2, \dots, y_h$ de h classes différentes $F_1, F_2, \dots, F_h$ tels que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h] = \frac{q^{k-h_1+1} - 1}{q - 1}$$

avec $h_1 \leq h$.

Dans ces conditions, on a :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h \cap y_0] = \frac{q^{k-h_1+1} - 1}{q - 1} \quad \text{ou} \quad \frac{q^{k-h_1} - 1}{q - 1}$$

Effectivement, utilisons e) : on peut extraire des plans $y_1, y_2, \dots, y_h$ h_1 plans $y_{\alpha_1}, y_{\alpha_2}, \dots, y_{\alpha_{h_1}}$ tels que :

$$\text{Card} [y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{h_1}}] = \frac{q^{k-h_1+1} - 1}{q - 1}$$

Dès lors, (propriété c) de définition des réseaux $(R)'$, on a :

$$\begin{aligned} \text{Card} [y_{\alpha_1} \cap y_{\alpha_2} \cap \dots \cap y_{\alpha_{h_1}} \cap y_0] &= \\ \text{soit } \frac{q^{k-h_1+1} - 1}{q - 1} &, \quad \text{soit } \frac{q^{k-h_1} - 1}{q - 1} . \end{aligned}$$

De même pour :

$$\text{Card } [y_1 \cap y_2 \cap \dots \cap y_h \cap y_o] .$$

Le nombre de points de $y_1 \cap y_2 \cap \dots \cap y_h$ dans le réseau (R) correspondant à (R)' sera donc égal :

soit à 0,

$$\text{soit à : } \frac{q^{k-h_1+1}-1}{q-1} - \frac{q^{k-h_1}-1}{q-1} = q^{k-h_1}$$

d'où l'on déduit facilement la propriété c) de définition des réseaux (R).

(β) Propriété d).

Utilisons la propriété d) de définition des réseaux (R)' :

Soient les classes de plans $F_1, F_2, \dots, F_h$ telles que :

$$\forall (y_1, y_2, \dots, y_h) \in F_1 \times F_2 \times \dots \times F_h$$

l'on ait :

$$\text{Card } [y_1 \cap y_2 \cap \dots \cap y_h] = \frac{q^{k-h+1}-1}{q-1}$$

Dans ce cas, nous allons vérifier la propriété suivante dans le réseau (R)' :

$$\text{Card } [y_1 \cap y_2 \cap \dots \cap y_h \cap y_o] = \frac{q^{k-h}-1}{q-1}$$

Remarquons tout de suite que cela est suffisant pour justifier la propriété d) de définition des réseaux (R) puisque dans ce cas, l'on a dans le réseau (R) :

$$\text{Card } [y_1 \cap y_2 \cap \dots \cap y_h] = \frac{q^{k-h+1}-1}{q-1} - \frac{q^{k-h}-1}{q-1} = q^{k-h}$$

Contentons-nous donc de vérifier la propriété énoncée. Nous allons la démontrer par récurrence : en effet, la propriété est exacte pour $h = 2$. Nous allons donc la supposer

vraie pour $h-1$ et voir qu'elle est encore vérifiée au rang h .

Pour cela, supposons par l'absurde que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h \cap y_0] = \frac{q^{k-h+1} - 1}{q - 1}$$

étant donnés $y_1, y_2, \dots, y_h$ tels que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1} \cap y_h] = \frac{q^{k-h+1} - 1}{q - 1}$$

Autrement dit : $y_1, y_2, \dots, y_h$ se coupent dans le plan y_0 , ce que l'on peut encore exprimer en disant que y_h passe par $y_1 \cap y_2 \cap \dots \cap y_{h-1} \cap y_0$.

Il est facile de vérifier en utilisant e) que :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1}] = \frac{q^{k-h} - 1}{q - 1}$$

Utilisant alors l'hypothèse de récurrence, on en déduit :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1} \cap y_0] = \frac{q^{k-h+1} - 1}{q - 1}$$

Soit alors x un point de $y_1 \cap y_2 \cap \dots \cap y_{h-1}$ n'appartenant pas à y_0 et soit y'_h le plan de F_h passant par x . De même que y_h , y'_h passe par $y_1 \cap y_2 \cap \dots \cap y_{h-1} \cap y_0$ (puisque $y'_h \subset y_h$).

Mais y'_h passe aussi par x .

Donc :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_{h-1} \cap y'_h] > \frac{q^{k-h+1} - 1}{q - 1}$$

Cela est impossible par hypothèse (propriété d) de définition des réseaux $(R)'$).

On aboutit donc à une contradiction : c'est que l'hypothèse de départ était absurde.

Finale ment :

$$\text{Card} [y_1 \cap y_2 \cap \dots \cap y_h \cap y_0] = \frac{q^{k-h} - 1}{q - 1}$$

c. q. f. d.

3) - Utilisation des quasi-groupes.

a) Théorème.

Soit X un ensemble de q éléments. Soit ϕ_j^i , $i \in [1, h]$, $j \in [1, k]$, ψ_i , $i \in [1, k]$, des lois de composition interne sur X , munissant chacune X d'une structure de quasi-groupe.

Supposons l'existence d'un élément a de X tel que :

$$\begin{cases} a \psi_i a = a & , \quad \forall i \in [1, k] \\ a \phi_1^i a \phi_2^i \dots \phi_k^i a = a & , \quad \forall i \in [1, h] \end{cases}$$

Soit, d'autre part, un groupe abélien de $q-1$ automorphismes α_i , $i \in [1, q-1]$, transitifs sur $X - \{a\}$ et tels que :

$$\alpha_i(a) = a \quad , \quad \forall i \in [1, q-1] .$$

Soit enfin l'application α_0 telle que :

$$\alpha_0(x) = a \quad , \quad \forall x \in X.$$

Etant donné le système I de $(h+k)q+1$ équations à $k+1$ inconnues $x_1, x_2, \dots, x_k$, suivant :

$$I \quad \left\{ \begin{array}{l} x_1 \phi_1^1 x_2 \phi_2^1 \dots \phi_k^1 \alpha^{i_1}(x_{k+1}) = a \quad , \quad \forall i_1 \in [0, q-1] \\ x_1 \phi_1^2 x_2 \phi_2^2 \dots \phi_k^2 \alpha^{i_2}(x_{k+1}) = a \quad , \quad \forall i_2 \in [0, q-1] \\ \dots \\ x_1 \phi_1^h x_2 \phi_2^h \dots \phi_k^h \alpha^{i_h}(x_{k+1}) = a \quad , \quad \forall i_h \in [0, q-1] \\ x_1 \psi_1 \alpha_{j_1}(x_{k+1}) = a \quad , \quad \forall j_1 \in [0, q-1] \\ x_2 \psi_2 \alpha_{j_2}(x_{k+1}) = a \quad , \quad \forall j_2 \in [0, q-1] \\ \dots \end{array} \right.$$

$$\left\{ \begin{array}{l} \dots \\ x_k \psi_k \alpha_{j_k}(x_{k+1}) = a \quad , \quad \forall j_k \in [0, q-1] \\ x_{k+1} = a \end{array} \right.$$

tel que :

(1) Tout système de deux équations à $k+1$ inconnues extrait de I admet q^{k-1} solutions.

(2) Tout système de 3 équations à $k+1$ inconnues extrait de I et du type suivant :

$$\left\{ \begin{array}{l} x_1 \phi_1^{j_1} x_2 \phi_2^{j_1} \dots \phi_k^{j_1} (\alpha_i(x_{k+1})) = a \\ x_1 \phi_1^{j_2} x_2 \phi_2^{j_2} \dots \phi_k^{j_2} (\alpha_j(x_{k+1})) = a \\ x_{k+1} = a \end{array} \right.$$

$\forall j_1 \neq j_2 \in [1, h] \quad , \quad \forall (i, j) \in [0, q-1]^2$, admet q^{k-2} solutions.

(3) Tout système de h équations, à $k+1$ inconnues extrait du système I admet :

- si $2 < h \leq k+1$: soit q^{k-1} , soit q^{k-2} , ...,
soit q^{k-h+1} solutions.
- si $h > k+1$: soit q^{k-1} , soit q^{k-2} , ...,
soit 1 solutions.

Alors, on peut faire correspondre à ces données un réseau $(R)^t$ à k dimensions.

Démonstration.

Les points du réseau $(R)^t$ sont les $k+1$ -tuples :
 $(x_1, x_2, \dots, x_{k+1})$, $x_i \in X$, $i \in [1, k+1]$, avec la convention suivante :

- le $(k+1)$ -tuple $(a, a, \dots, a)$ est exclus;
- les $(k+1)$ -tuples $(x_1, x_2, \dots, x_{k+1})$ et :

$$\alpha_i(x_1, x_2, \dots, x_{k+1}) = [\alpha_i(x_1), \alpha_i(x_2), \dots, \alpha_i(x_{k+1})]$$

$\forall i \in [1, q-1]$ sont identifiés à un point.

Avec cette convention, on aura $\frac{q^{k+1}-1}{q-1}$ points différents dans le réseau (R)' construit, puisque les automorphismes α_i sont transitifs sur $X - \{a\}$.

Les plans du réseau (R)' sont représentés chacun par une équation, soit :

$$- x_1 \phi_1^j x_2 \phi_2^j \dots \phi_k^j \alpha_i(x_{k+1}) = a$$

$\forall j \in [1, h]$, $\forall i \in [0, q-1]$, ce qui donne en tout hq plans.

$$- x_j \psi_j \alpha_i(x_{k+1}) = a$$

$\forall j \in [1, k]$, $\forall i \in [0, q-1]$, ce qui donne en tout kq plans.

$$- x_{k+1} = a \quad \text{enfin joue le rôle du plan } y_0.$$

On construit ainsi $q(h+k)+1$ plans.

Il reste à vérifier sur ces données les propriétés de définition des réseaux (R)'.

Nous pouvons tout de suite remarquer que chaque plan ainsi construit contient $\frac{q^k-1}{q-1}$ points.

- Considérons tout d'abord le plan $x_{k+1} = a$.
 $x_1 x_2 \dots x_k$ sont quelconques, d'où q^k possibilités. Mais le point $(a, a, \dots, a)$ est exclus et $(x_1, x_2, \dots, x_{k+1})$ est confondu avec $\alpha_i(x_1, x_2, \dots, x_{k+1})$, $\forall i \in [1, q-1]$.

D'où finalement :

$$\frac{q^k-1}{q-1} \text{ points.}$$

- Considérons ensuite le plan : $x_i \psi_i \alpha_j(x_{k+1}) = a$.
 De chaque valeur de x_{k+1} , on déduit une solution et une seule de l'équation $x_i \psi_i \alpha_j(x_{k+1}) = a$ en x_i et ceci

bien sûr, $\forall (x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_k)$, soient donc au total q^k possibilités.

Mais si (x_i, x_{k+1}) est solution de $x_i \psi_i \alpha_j(x_{k+1}) = a$ $\alpha_1(x_i, x_{k+1})$ est aussi solution de la même équation $\forall i \in [1, q-1]$, puisque les α_1 forment un groupe transitif d'automorphismes sur $X - \{a\}$, tels que $\alpha_1(a) = a$:

$$\alpha_1(x_i \psi_i \alpha_j(x_{k+1})) = \alpha_1(a) = a = \alpha_1(x_i) \psi_i \alpha_j \alpha_1(x_{k+1})$$

D'autre part, $(a, a, \dots, a)$ est exclus et (a, a) est solution puisque :

$$a \psi_i a = a.$$

On obtient donc encore une fois $\frac{q^k - 1}{q - 1}$ points.

- Considérons enfin le plan d'équation :

$$x_1 \phi_1^i x_2 \phi_2^i \dots \phi_k^i \alpha_j(x_{k+1}) = a$$

C'est exactement la même chose que précédemment. On a : q^k solutions.

On a :

$$a \phi_1^i a \phi_2^i \dots \phi_k^i a = a$$

On a :

$$\alpha_1(x_1 \phi_1^i \dots \phi_k^i \alpha_j(x_{k+1})) = \alpha_1(a) =$$

$$\alpha_1(x_1) \phi_1^i \dots \phi_k^i \alpha_j \alpha_1(x_{k+1}) = a$$

Soit finalement :

$$\frac{q^k - 1}{q - 1} \text{ points.}$$

Passons enfin à la vérification des propriétés de définition des réseaux (R)'.

(1) Nous devons tout d'abord exhiber une relation d'équivalence S entre les plans ainsi construits.

Ce sera la suivante :

Deux plans y_i et y_j seront en relation S, $y_i S y_j$, si et seulement si les équations de y_i et y_j sont :

$$(a) \quad \begin{cases} x_1 \phi_1^j & x_2 \phi_2^j & \dots & \phi_k^j & \alpha_{i_1}(x_{k+1}) = a \\ \text{et :} \\ x_1 \phi_1^j & x_2 \phi_2^j & \dots & \phi_k^j & \alpha_{i_2}(x_{k+1}) = a, \end{cases}$$

ou bien encore si les équations de y_i et y_j sont du type suivant :

$$(ab) \quad \begin{cases} x_i \psi_i & \alpha_{i_1}(x_{k+1}) = a \\ \text{et} \\ x_i \psi_i & \alpha_{i_2}(x_{k+1}) = a. \end{cases}$$

($\alpha_{i_1} \neq \alpha_{i_2}$ étant tous deux fixés).

Il est facile de vérifier que la relation S ainsi définie est une relation d'équivalence et que c'est la relation d'équivalence de définition des réseaux (R)', à savoir que deux plans en relation S se coupent dans y_0 d'équation $x_{k+1} = a$.

En effet, si $x_{k+1} \neq a$, (a) ou (b) ne peuvent avoir de solution en $(x_1 \ x_2 \ \dots \ x_{k+1})$ puisqu'alors :

$$\alpha_{i_1}(x_{k+1}) \neq \alpha_{i_2}(x_{k+1})$$

(les automorphismes étant transitifs sur $X - \{a\}$).

Il n'y aura de solution possible que si $x_{k+1} = a$. On sait qu'alors :

$$\alpha_i(x_{k+1}) = a \quad \forall i \in [1, q-1].$$

Il est facile de constater que si les équations de y_i et y_j ne sont pas des types (a) ou (b), y_i et y_j ne peuvent se couper seulement dans y_0 , donc ne sont pas en relation S.

Ainsi prenons par exemple deux plans y_i et y_j d'équations :

$$x_1 \phi_1^i \ x_2 \phi_2^i \ \dots \ \phi_k^i \ \alpha_{i_1}(x_{k+1}) = a$$

$$x_1 \phi_1^j \ x_2 \phi_2^j \ \dots \ \phi_k^j \ \alpha_{i_2}(x_{k+1}) = a$$

Adjoignons à ces deux équations où $i \neq j$, la troisième équation $x_{k+1} = a$.

Le système ainsi constitué de trois équations à $k+1$ inconnues admet par hypothèse q^{k-2} solutions, alors que le système primitif de 2 équations à $k+1$ en admettait q^{k-1} .

D'où $q^{k-2}(q-1)$ solutions pour lesquelles $x_{k+1} \neq a$.

Soit finalement q^{k-2} points d'intersection pour y_i et y_j qui n'appartiennent pas à y_0 . (Effectivement, on a vu que si $(x_1 \ x_2 \ \dots \ x_{k+1})$ est solution d'une équation quelconque extraite de $\mathbb{I}$, $\alpha_i(x_1, x_2, \dots, x_{k+1})$ est aussi solution de cette même équation $\forall i \in [1, q-1]$; on doit donc diviser $q^{k-2}(q-1)$ par $q-1$).

(2) Les propriétés a, b, et e de définition des réseaux (R)' sont ensuite aisément vérifiables et nous nous contenterons seulement de vérifier les propriétés c) et d).

Propriété c) de définition.

Par hypothèse, dans l'énoncé du théorème, nous savons que tout système de h équations à $k+1$ inconnues extrait du système I, admet :

- si $2 < h \leq k+1$:

soit q^{k-1} , soit q^{k-2} , ..., soit q^{k-h+1} solutions.

- si $h > k+1$:

soit q^{k-1} , soit q^{k-2} , ..., soit 1 solutions.

Ce qui se traduit en langage géométrique par :
 h plans quelconques du réseau (R) se coupent en :

- $\frac{q^{k-1}-1}{q-1}$ ou $\frac{q^{k-2}-1}{q-1}$ ou ... ou $\frac{q^{k-h+1}-1}{q-1}$ points,

si $2 < h \leq k+1$

- $\frac{q^{k-1}-1}{q-1}$ ou $\frac{q^{k-2}-1}{q-1}$ ou ... ou 0 points ,

si $h > k$

C'est ce qui constitue la propriété c) de définition

c. q. f. d.

Propriété d) de définition.

Les k classes ^{de plans} que nous retiendrons sont les suivantes :

$$\left\{ \begin{array}{ll} x_1 \quad \psi_1 \quad \propto i_1(x_{k+1}) = a & \forall i_1 \in [0, q-1] \\ x_2 \quad \psi_2 \quad \propto i_2(x_{k+1}) = a & \forall i_2 \in [0, q-1] \\ \dots & \\ x_k \quad \psi_k \quad \propto i_k(x_{k+1}) = a & \forall i_k \in [0, q-1] \end{array} \right.$$

Considérons h plans quelconques appartenant aux h premières classes, par exemple :

$$\left\{ \begin{array}{l} x_1 \quad \psi_1 \quad \alpha_{i_1}(x_{k+1}) = a \\ x_2 \quad \psi_2 \quad \alpha_{i_2}(x_{k+1}) = a \\ \dots \\ x_h \quad \psi_h \quad \alpha_{i_h}(x_{k+1}) = a \end{array} \right.$$

En fixant x_{k+1} n'importe comment dans X , on obtient une solution et une seule en $x_1, x_2, \dots, x_h$. D'où q solutions pour le système envisagé, soit q^{k+1-h} possibilités pour le $k+1$ -tuple $(x_1, x_2, \dots, x_{k+1})$ et finalement donc

$$\frac{q^{k+1-h} - 1}{q - 1}$$

points d'intersection pour les h plans considérés.

La propriété d) de définition en découle aisément.

c. q. f. d.

Remarques.

α) Vu que $\alpha_o(x) = a$, $\forall x \in X$ et puisque :
 $a \psi_i a = a$, $a \phi_1^i a \phi_2^i \dots \phi_k^i a = a$,
 il est bien certain que α_o est aussi un automorphisme.

β) Nous n'avons pas insisté sur l'écriture particulière des plans de la forme :

$$x_i \quad \psi_i \quad \alpha_o(x_{k+1}) = a$$

ou de la forme :

$$x_1 \phi_1^i x_2 \phi_2^i \dots \phi_k^i \alpha_o(x_{k+1}) = a$$

Ces équations peuvent aussi bien s'écrire :

$$x_i \psi_i a = a$$

$$(d'où \quad x_i = a)$$

et :

$$x_1 \phi_1^i x_2 \phi_2^i \dots \phi_k^i a = a$$

Il est bien évident que cette écriture ne pose aucun problème.

b) Nous avons vu comment construire un réseau (R) à partir d'un réseau (R)'.

Il est bien certain qu'à partir des données du théorème précédent, l'on peut construire un réseau (R). La démonstration directe de ce résultat tout en étant assez longue, ne pose aucun problème et elle est inutile, vu IV. A. 2. g.

Il s'agit de supprimer le plan y_0 . On doit donc supposer $x_{k+1} \neq a$.

Les points du réseau (R) sont alors identifiés aux k-tuples $(x_1, x_2, \dots, x_k)$.

Les plans du réseau (R) sont les suivants :

$$- x_i = a_j \quad \forall i \in [1, k] \quad , \quad \forall a_j \in X.$$

$$- x_1 \phi_1^i x_2 \phi_2^i \dots \phi_{k-1}^i x_k = a_j \quad ,$$

$$\forall i \in [1, h] \quad , \quad \forall a_j \in X$$

soient donc $h+k$ classes de q plans.

Effectivement, soient les plans :

$$x_1 \psi_1 \varphi_i(x_{k+1}) = a \quad \forall i \in [0, q-1]$$

On a $x_{k+1} \neq a$, donc $\alpha_i(x_{k+1})$ décrit X quand i varie ;
autrement dit, x_1 décrit également X . On obtient donc
ainsi la classe de plans :

$$x_1 = a_i \quad \forall a_i \in X$$

De même les plans :

$$x_1 \phi_1^i x_2 \phi_2^i \dots \phi_k^i \alpha_i(x_{k+1}) = a$$

$$\forall i \in [0, q-1],$$

conduisent à la classe de plans :

$$x_1 \phi_1^i x_2 \phi_2^i \dots \phi_{k-1}^i x_{k-1} = a_i$$

$$\forall a_i \in X.$$

B) - Les réseaux $(R)''$.

1) - L'étude des réseaux $(R)'$ peut être intéressante puisque la connaissance d'un réseau $(R)'$ permet de construire un réseau (R) par suppression d'un plan.

Nous allons compléter cette étude par celle du plan y_0 que l'on ôte de $(R)'$, ce qui nous amènera à définir une structure de réseau $(R)''$ (qui sera donc celle du plan y_0).

D'un réseau $(R)'$, on déduira donc un réseau (R) et un réseau $(R)''$ dont $(R)'$ sera en quelque sorte la réunion.

Nous n'étudierons pas en détail les réseaux $(R)''$, étant donné qu'il ne semble pas que l'on puisse déduire de réseaux (R) de la connaissance d'un réseau $(R)''$.

2) - Définition des réseaux $(R)''$.

Soit E un ensemble fini d'éléments désignés par des points.

Soit F un ensemble fini d'éléments désignés par des plans.

Soit R un sous-ensemble de $E \times F$.

Soient q et k , deux nombres entiers positifs.

Le système $(E, F, R, q, k-1)$ définit un réseau $(R)^n$ de dimension $k-1$, si l'on a les propriétés suivantes de définition :

a) $\forall (y_1, y_2) \in F^2$, $y_1 \neq y_2$, on a :

$$\text{Card} [x : x \in E \text{ , } (x, y_1) \in R \text{ , } (x, y_2) \in R] = \frac{q^{k-2} - 1}{q - 1}$$

b) $\forall (y_1, y_2, \dots, y_h) \in F^h$, $y_1 \neq y_2 \neq \dots \neq y_h$:

$$\text{Card} [x : x \in E \text{ , } (x, y_1) \in R, (x, y_2) \in R, \dots, (x, y_h) \in R] =$$

$$\alpha) \text{ soit } \frac{q^{k-2} - 1}{q - 1} \text{ , soit } \frac{q^{k-3} - 1}{q - 1} \text{ , } \dots \text{ , soit } \frac{q^{k-h} - 1}{q - 1}$$

$$\text{si } 2 < h \leq k$$

$$\beta) \text{ soit } \frac{q^{k-2} - 1}{q - 1} \text{ , soit } \frac{q^{k-3} - 1}{q - 1} \text{ , } \dots \text{ , soit } 1 \text{ , soit } 0$$

$$\text{si } h > k.$$

c) Il existe $(y_1, y_2, \dots, y_{k-1}) \in F^{k-1}$, $y_1 \neq y_2 \neq \dots \neq y_{k-1}$, tels que :

$$\text{Card} [x ; (x, y_{i_1}) \in R, (x, y_{i_2}) \in R, \dots, (x, y_{i_h}) \in R] = \frac{q^{k-h} - 1}{q - 1}$$

$$\forall h \in [2, k-1] .$$

$$\forall (i_1, i_2, \dots, i_h) \in [1, k-1]^h \text{ , } i_1 \neq i_2 \neq \dots \neq i_h.$$

$$d) \quad \forall y \in F, \text{Card} [x : x \in E, (x, y) \in R] = \frac{q^{k-1} - 1}{q - 1}$$

$$e) \text{Card} [E] = \frac{q^k - 1}{q - 1}$$

3) - Il est facile de vérifier que ce sont là les propriétés du plan y_0 de $(R)'$. Une étude des réseaux $(R)''$ commencerait par l'énoncé de la propriété :

L'application f de F dans $P(E)$:

$$\forall y \in F, f(y) = \{x : x \in E, (x, y) \in R\}$$

est injective.

Cela conduirait à remplacer chaque plan par la partie de E correspondante et à étudier le système ainsi obtenu.

REFERENCES :

- [1] - Bose R. C. Shrikhande S. S. Trans. Amer. Math. Soc. 95 (1960), p. 191-207.
- [2] - Bose R. C. Shrikhande S. S. Parker. Canadian. J. Math. 12. (1960), p. 189-203.
- [3] - Lecointe P. C. R. Ac. des Sc. Paris. (à paraître).
- [4] - Guérin. Existence et Propriétés des carrés latins orthogonaux. Thèse. 1965.

C H A P I T R E VI

Treillis associés à des réseaux (R) et des Systèmes de Plans (S_k).

I. Introduction.

La théorie des treillis a été utilisée dans l'étude des géométries projectives et affines généralisées ([1]). De façon analogue, on peut associer une axiomatique de treillis aux réseaux (R) et aux systèmes de plans (S_k). Après avoir rappelé quelques résultats classiques, nous développerons la théorie des réseaux et des systèmes de plans sous cette optique.

II. Rappels algébriques ([1]).

1) - Définitions et propriétés.

- Un élément p d'un treillis (T) à élément nul 0 est un point si cet élément couvre l'élément nul.

- Un treillis (T) à élément nul est atomique si pour tout élément x différent de 0 , il existe un point p contenu dans x .

- Un treillis (T) vérifie la condition (c) si tout segment $[a, b]$ du treillis (T) est atomique.

- Une chaîne reliant deux éléments d'un treillis est maximale si un élément n'en faisant pas partie ne peut y être intercalé.

- Si dans un treillis, toute suite d'éléments $a_1, a_2, \dots, a_n, \dots$ telle que $a_1 < a_2 < \dots < a_n < \dots$, est finie, le treillis vérifie la condition de chaîne ascendante.

- De même, si dans un treillis, toute suite d'éléments $a_1 \dots a_n \dots$ telle que : $a_1 > a_2 > \dots > a_n > \dots$, est finie, le treillis vérifie la condition de chaîne descendante.

- On dira, dans un treillis, que toutes les chaînes bornées sont de longueur finie, si tout segment satisfait à la condition de chaîne ascendante et à la condition de chaîne descendante.

- La longueur d'une chaîne de n éléments est par définition égale à $n-1$.

- La hauteur d'un élément x , soit $h(x)$, est égale au maximum s'il existe des longueurs de chaînes admettant x comme élément maximum.

- Un treillis vérifie la condition de chaîne de Jordan-Dedekind si les chaînes maximales joignant deux éléments fixes quelconques ont même longueur.

- Un treillis (T) vérifie l'égalité (E) si $\forall x, y \in (T)$:

$l[y, x \cup y] = l[x \cap y, x]$, $l(a,b)$ désignant la longueur de toutes les chaînes maximales joignant a et b .

(Le treillis (T) vérifie donc par hypothèse la condition de chaîne de Jordan-Dedekind).

- Un treillis (T) est semi-modulaire inférieurement si :

$$\forall A \succ B, A \succ C, B \neq C \implies \begin{cases} B \succ B \cap C \\ C \succ B \cap C \end{cases}$$

On en déduit ainsi que ^{si} dans un treillis (T) vérifiant

la condition de chaîne ascendante on a :

$$x \cup y \succ x \implies y \succ x \cap y ,$$

le treillis (T) est semi-modulaire inférieurement.

- De même, un treillis (T) est semi-modulaire supérieurement si :

$$\left. \begin{array}{l} \forall \left. \begin{array}{l} A \prec B \\ A \prec C \\ B \neq C \end{array} \right\} \implies \left\{ \begin{array}{l} C \cup B \succ B \\ C \cup B \succ A \end{array} \right.$$

Il est alors facile de voir qu'un treillis (T) vérifiant la condition (c) et tel que :

$$y \succ x \cap y \implies x \cup y \succ x \quad (1)$$

est semi-modulaire supérieurement

- Un treillis est modulaire s'il est à la fois, semi-modulaire inférieurement et semi-modulaire supérieurement.

- Un treillis dans lequel toutes les chaînes bornées sont de longueur finie, vérifiant la condition de chaîne de Jordan-Dedekind et l'égalité (E) est modulaire.

- Un treillis est modulaire affaiblie s'il possède un élément nul et s'il satisfait à la condition suivante :

$$x \leq z \text{ et } y \cap z \neq 0 \implies x \cup (y \cap z) = (x \cup y) \cap z$$

- Un élément x' satisfaisant à :

$$\begin{cases} x \cap x' = 0 \\ x \cup x' = u \end{cases}$$

(1) La condition (c) peut être remplacée par la condition de chaîne descendante.

(0 élément nul du treillis, u élément universel du treillis) est appelé un complément de x.

- Un treillis avec élément nul et élément universel dans lequel tout élément admet au moins un complément est dit complémenté.

- Un élément x'satisfaisant à :

$$\begin{cases} x \cap x' = a \\ x \cup x' = b \end{cases}$$

est appelé complément relatif de x par rapport à a et b.

- Un treillis dans lequel pour tout couple d'éléments (a,b) tels que $a \leq b$, tout élément du segment (a, b) admet au moins un complément relatif par rapport à a et b est dit relativement complémenté.

- Un treillis est distributif si l'on a la condition supplémentaire suivante :

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z).$$

- Deux treillis S et T sont isomorphes s'il existe un isomorphisme de T sur S = $\alpha(T)$, c'est-à-dire une application biunivoque telle que l'on ait la propriété : $x \leq y$ dans T est équivalente à $\alpha(x) \leq \alpha(y)$ dans $\alpha(T)$.

- Soit T_α , $\alpha \in A$ une famille de treillis. Alors le produit cardinal général est un treillis T :

Deux éléments $x = \{x_\alpha\}_{\alpha \in A}$ et $y = \{y_\alpha\}_{\alpha \in A}$ de T ayant une union donnée par :

$$x \cup y = \{x_\alpha \cup y_\alpha\}_{\alpha \in A}$$

et une intersection donnée par :

$$x \cap y = \{x_\alpha \cap y_\alpha\}_{\alpha \in A}.$$

- Un treillis est dit irréductible s'il n'est d'aucune façon isomorphe au produit cardinal de treillis ayant plus d'un élément.

- Soit un sous-ensemble S d'un treillis (T) :

a) On dit qu'un élément x de S est U -dépendant d'un ensemble $\{x_\alpha\}_{\alpha \in A}$ fini ou infini d'éléments de S si x est inférieur ou égal à l'union d'un nombre fini de ces éléments. On dit aussi que x est U -dépendant des éléments x_α .

b) On dit qu'un ensemble $\{x_\alpha\}_{\alpha \in A}$ d'éléments de S forme une famille libre (U -indépendance) si chaque élément x_α est U -indépendant de l'ensemble des autres.

c) Etant donné un ensemble $\{x_\alpha\}_{\alpha \in A}$ d'éléments de S , on appelle base de cet ensemble une famille libre qui en est extraite et telle que tous les éléments de $\{x_\alpha\}_{\alpha \in A}$ en soient U -dépendants.

d) Théorème de la base incomplète.

Si tous les éléments d'un ensemble $E = \{x_\alpha\}_{\alpha \in A}$ d'éléments de S sont U -dépendants d'un nombre fini d'entre eux, toute famille libre extraite de E est finie et si $\{x_i\}_{i=1, 2, \dots, n}$ constitue une telle famille libre, il existe une base de E contenant tous les éléments x_i .

e) Théorème du rang.

Si tous les éléments d'un ensemble $E \subset S$ sont U -dépendants d'un nombre fini d'entre eux $\{x_i\}_{i \in [1, n]}$ toutes les bases de E ont même nombre fini d'éléments n . (Les éléments de E sont de rang n).

2) - Treillis Géométriques de dimension finie n.

Axiome 1 :

Les variétés linéaires sont les éléments d'un treillis avec élément nul et élément universel.

Axiome 2 :

Loi de couverture : Si P est un point non situé dans B, la variété $B \cup P$ couvre B.

Axiome 3 :

L'ensemble des points situés dans toute variété $A \neq 0$ n'est pas vide et A est l'union d'un nombre fini d'entre eux.

Définition.

On appelle treillis géométrique de dimension n un treillis vérifiant les axiomes 1, 2 et 3 tel que la dimension de l'élément universel soit égale à n.

Remarques.

a) Une variété A union de k de ses points $x_1, x_2, \dots, x_k$ sera dite de dimension k-1. Les points de A sont alors U-dépendants de $x_1, x_2, \dots, x_k$ qui constituent une base de A (famille libre d'éléments de A).

b) Un plan d'un treillis est un élément couvert par l'élément universel.

- Les treillis géométriques vérifient la réciproque de la loi de couverture :

$$\forall A \succ B \quad \exists P \notin B \implies A = B \cup P$$

(P désigne un point).

- Ce sont d'autre part, des treillis dans lesquels

la condition (c) est vérifiée et pour lesquels :

$$y \succ x \cap y \implies x \cup y \succ x.$$

Les treillis géométriques sont donc en particulier des treillis semi-modulaires supérieurement.

- Il est donc aisé d'établir la propriété caractéristique suivante :

Pour qu'un treillis soit un treillis géométrique de dimension n , il faut et il suffit qu'il soit semi-modulaire supérieurement de longueur finie $n+1$ et relativement complété.

3) - Géométries Projectives de dimension n .

Axiome 4 :

Loi duale de la loi de couverture.

Si A n'est pas contenu dans le plan H , il couvre $A \cap H$.

Définition.

On appelle treillis projectif de dimension n ou géométrie projective de dimension n un treillis géométrique de dimension n vérifiant l'axiome 4.

Il est facile de déduire de l'axiome 4, en particulier, que les treillis projectifs sont semi-modulaires inférieurement. Il en résulte la propriété caractéristique :

Un Treillis est une géométrie projective de dimension n si et seulement si c'est un treillis de longueur finie $n+1$ modulaire et complété.

Remarque.

La notion classique de géométrie projective correspond à celle de Treillis projectif irréductible.

4) - Géométrie Projectives affaiblies.

Axiome 4. a.

Si A n'est pas contenu dans le plan H , il couvre $A \cap H$ lorsque $A \cap H \neq \emptyset$.

Définition.

On appelle treillis géométrique affaibli ou géométrie projective affaiblie tout treillis géométrique vérifiant l'axiome 4. a.

Il est facile de voir que tout segment $[X, U]$, $X \neq \emptyset$, issu d'une géométrie projective affaiblie est une géométrie projective, tout segment $[X, U]$ étant modulaire.

D'autre part, tout segment $(\emptyset, A)$, $A \neq \emptyset$, issu d'une géométrie projective affaiblie est une géométrie projective affaiblie.

Remarquons une construction qui sera intéressante pour les géométries affines. Soit une géométrie projective irréductible. Si l'on ôte de cette géométrie une variété A , on obtient une géométrie projective affaiblie.

5) - Géométries Affines.

Définissons tout d'abord la notion de parallélisme. A est parallèle à B ($A \parallel B$) lorsque les deux conditions suivantes sont remplies :

$$- A \cap B = \emptyset$$

$$- A \cup B > A.$$

Pour que deux variétés A et B d'un treillis géométrique de dimension finie soient parallèles, il faut et il suffit :

$$A \parallel B \quad \text{et} \quad d[A] = d[B]$$

Postulat d'Euclide.

Etant donnés une droite D d'un treillis géométrique et un point $P \notin D$, il existe une droite X et une seule passant par P telle que X et D soient parallèles.

Définition.

On appelle treillis affine ou géométrie affine une géométrie modulaire affaiblie de dimension au moins égale à 2 vérifiant le postulat d'Euclide.

Remarque.

Une droite est une variété à une dimension, donc définie par deux points.

La construction d'une géométrie affine s'effectue à partir d'une géométrie projective irréductible de la façon suivante :

On ôte de cette dernière un plan, le treillis restant est celui d'une géométrie affine.

D'autre part, on peut démontrer que le parallélisme est une relation d'équivalence entre variétés.

On a enfin la construction réciproque de la précédente, celle d'une géométrie projective irréductible à partir d'une géométrie affine.

(référence [1] page 311)

La propriété caractéristique d'une géométrie affine est celle de sa définition. Le treillis est ici d'une nature plus complexe que dans les deux premiers cas simples des treillis géométriques et projectifs.

III. Treillis associé à un réseau (R).

1) - Axiomes de définition des treillis ($\mathcal{C}$).

Axiome 1.

Les variétés sont les éléments d'un treillis avec élément nul 0 et élément universel u.

Axiome 2.

(Loi faible de couverture).

Pour toute variété $A \neq 0$, il existe un point P n'appartenant pas à A, tel que la variété $A \cup P$ couvre A.

$$\forall A \exists P \Rightarrow A \cup P \succ A.$$

Axiome 3.

(Loi duale affaiblie).

Pour toute variété $A \neq 0$ n'appartenant pas à un plan H, telle que $A \cap H$ ne soit pas vide, A couvre $A \cap H$.

$$\forall A \not\subseteq H, A \cap H \neq 0 \Rightarrow A \succ A \cap H.$$

Axiome 4.

Aucune variété n'est vide et toute variété est l'union d'un nombre fini de ses points (y compris l'élément universel u).

En outre, pour toute variété A (y compris u), il existe des points $P_1, P_2, \dots, P_{d+1}$, tels que :

$$A = \bigcup_{i \in [1, d+1]} P_i \quad \text{et :} \quad (\bigcup_{i \in I} P_i) \cup P_k \succ (\bigcup_{i \in I} P_i)$$

$$\forall I \subset [1, d+1], \forall k \neq I.$$

(Le nombre d+1 est fixé par la variété A).

Axiome 5.

(Réciproque de la loi duale de couverture).

Pour toute variété A couvrant B , il existe un plan H , tel que B soit égale à $A \cap H$.

$$\forall A \rangle_B \exists H \iff B = A \cap H.$$

Axiome 6.

(Postulat d'Euclide).

Par tout point, il passe un plan et un seul, parallèle à un plan donné.

Axiome 7.

Pour toute variété $A \neq 0$, pour tous plans H_1 et H_2 , tels que :

$$A \rangle A \cap H_1 \quad \text{et} \quad H_1 \cap H_2 = 0$$

on a :

$$A \rangle A \cap H_2.$$

Remarques.

(a) Dans la suite, la notation :

- P , sera réservée aux points de $(\mathcal{L})$.
- A , sera réservée aux variétés de $(\mathcal{L})$,
- (d'une façon générale).
- H , sera réservée aux plans de $(\mathcal{L})$.

(b) Le Postulat d'Euclide est énoncé ici pour des plans. On dira que deux plans H_1 et H_2 sont parallèles si et seulement si $H_1 \cap H_2 = 0$.

Il est facile de constater que la relation de parallélisme entre plans :

$$H_1 \parallel H_2 \iff H_1 \cap H_2 = 0 \quad \text{ou} \quad H_1 = H_2$$

est une relation d'équivalence (par application du Postulat d'Euclide).

Nous reviendrons sur la notion de parallélisme dans un treillis ($\mathcal{L}$) au paragraphe suivant.

(c) Soient h plans $H_1, H_2, \dots, H_h$ tels que :

$$(1) \quad H_1 \succ H_1 \cap H_2 \succ H_1 \cap H_2 \cap H_3 \succ \dots \succ H_1 \cap H_2 \cap \dots \cap H_h \neq 0$$

On a :

$$(2) \quad H_{i_1} \succ H_{i_1} \cap H_{i_2} \succ H_{i_1} \cap H_{i_2} \cap H_{i_3} \succ \dots \succ H_{i_1} \cap H_{i_2} \cap \dots \cap H_{i_h} \neq 0$$

pour toute permutation $(i_1, i_2, \dots, i_h)$ de $(1, 2, \dots, h)$.

Démonstration.

Ce résultat découle immédiatement de l'axiome 3.

Nous allons le démontrer par récurrence.

- On considère tout d'abord le cas $h = 3$.

On a donc :

$$H_1 \succ H_1 \cap H_2 \succ H_1 \cap H_2 \cap H_3 \neq 0$$

$H_1 \cap H_2 \cap H_3 \neq 0$ impliquent que les 3 plans H_1, H_2, H_3 ne

sont pas parallèles. On a donc :

$$H_{i_1} \succ H_{i_1} \cap H_{i_2} \quad \forall i_1 \neq i_2, (i_1, i_2) \in [1, 2, 3]^2$$

Supposons par l'absurde que :

$$H_1 \cap H_3 = H_1 \cap H_2 \cap H_3$$

(Autrement dit, le plan H_2 passe par H_1 et H_3). On aurait

alors :

$$H_1 \cap H_2 \succ H_1 \cap H_3.$$

On aurait donc à la fois :

$$H_1 \succ H_1 \cap H_2 \succ H_1 \cap H_3 \quad \text{et} \quad H_1 \succ H_1 \cap H_3$$

ce qui est impossible.

Donc $H_1 \cap H_3 > H_1 \cap H_2 \cap H_3$ (axiome 3) et la propriété énoncée suit aisément pour $n = 3$.

- Supposons la propriété vérifiée pour $n-1$ plans $H_1, H_2, \dots, H_{n-1}$ et ajoutons un plan H_n , tel que :

$$(1) H_1 > H_1 \cap H_2 > \dots > H_1 \cap H_2 \cap \dots \cap H_n \neq 0$$

Remarquons que puisque $H_1 \cap H_2 \cap \dots \cap H_n \neq 0$, les plans $H_1, H_2, \dots, H_n$ ne sont pas parallèles.

D'autre part, vue la relation (1), le plan H_n ne passe pas par $H_1 \cap H_2 \cap \dots \cap H_{n-1}$; donc il ne passe pas à fortiori par $H_1 \cap H_2 \cap \dots \cap H_{n-1}$, $\forall i_1 \neq i_2 \neq \dots \neq i_{n-1}, (i_1, i_2, \dots, i_{n-1}) \in [1, n-1]^{n-1}$

Supposons alors par l'absurde que :

$$(3) H_1 \cap H_2 \cap \dots \cap H_{n-1} = H_1 \cap H_2 \cap \dots \cap H_{n-1} \cap H_n$$

$$(n_1 \leq n, \quad i_1 \neq i_2 \neq \dots \neq i_{n-1}, (i_1, i_2, \dots, i_{n-1}) \in [1, n]^{n-1})$$

3 cas sont possibles.

$$\alpha) i_{n-1} = n, \text{ c'est-à-dire } H_{i_{n-1}} = H_n$$

La relation (3) est impossible puisque, en vertu de (1), H_n ne peut passer par $H_1 \cap H_2 \cap \dots \cap H_{n-1}$.

On a donc :

$$H_1 \cap H_2 \cap \dots \cap H_{n-1} > H_1 \cap H_2 \cap \dots \cap H_{n-1} \cap H_n$$

(en appliquant l'axiome 3).

de h. $\theta) i_1, i_2, \dots, i_{h_1}$, sont tous différents

Par récurrence, (3) est impossible et on a :

$$H_{i_1} \cap \dots \cap H_{i_{h_1-1}} > H_{i_1} \cap \dots \cap H_{i_{h_1}}$$

$\theta) i_1$ par exemple est égal à h.

(3) s'écrit :

$$H_h \cap H_{i_2} \cap \dots \cap H_{i_{h_1-1}} = H_h \cap H_{i_2} \cap \dots \cap H_{i_{h_1}}$$

Or on a :

$$H_{i_2} \cap \dots \cap H_{i_{h_1-1}} > H_{i_2} \cap \dots \cap H_{i_{h_1-1}} \cap H_h$$

(axiome 3)

et :

$$H_{i_2} \cap \dots \cap H_{i_{h_1-1}} > H_{i_2} \cap \dots \cap H_{i_{h_1}}$$

(récurrence)

et :

$$H_{i_2} \cap \dots \cap H_{i_{h_1}} > H_{i_2} \cap \dots \cap H_{i_{h_1}} \cap H_h$$

(axiome 3)

c'est-à-dire :

$$H_{i_2} \cap \dots \cap H_{i_{h_1-1}} > H_{i_2} \cap \dots \cap H_{i_{h_1-1}} \cap H_h$$

et :

$$H_{i_2} \cap \dots \cap H_{i_{h_1-1}} > H_{i_2} \cap \dots \cap H_{i_{h_1}} \cap H_h$$

avec :

$$H_{i_2} \cap \dots \cap H_{i_{h_1-1}} \cap H_h = H_{i_2} \cap \dots \cap H_{i_{h_1-1}} \cap H_h$$

ce qui est impossible. On en déduit en appliquant l'axiome 3 :

$$H_{i1} \cup H_{i2} \cup \dots \cup H_{i h_1 - 1} > H_{i1} \cup \dots \cup H_{i h_1}$$

et la propriété énoncée est démontrée.

2) - Propriétés des Treillis ($\mathcal{K}$).

a) Réciproque de la loi de couverture.

Les treillis ($\mathcal{K}$) vérifient la réciproque de la loi de couverture :

$$\forall A > B, \exists P \implies A = B \cup P.$$

Cette propriété est entraînée par l'axiome 4. Soient A et B deux variétés, telles que : $A > B$.

Par application de l'axiome 4, on sait que :

$$A = \bigcup P_i \quad \text{et} \quad B = \bigcup P'_i$$

$i \in [1, d+1] \quad \text{et} \quad i \in [1, d'+1]$

Puisque $A > B$, il existe au moins un point P_i , tel que :

$$P_i \in A \quad \text{et} \quad P_i \notin B$$

On a alors :

$$B \cup P_i > B \quad \text{et} \quad B \cup P_i \subset A$$

$$\text{Donc : } A = B \cup P_i$$

$$b) \quad \overline{\forall A, \exists H \iff A > A \cap H}$$

Soit une variété A. On a (axiome 4) :

$$A = P_1 \cup P_2 \cup \dots \cup P_{d+1}$$

Soit alors : $A' = P_1 \cup P_2 \cup \dots \cup P_d$

On a : $A' \not> A'$ (axiome 4).

Donc il existe un plan H , tel que :

$$A' = A \cap H$$

(ceci en vertu de l'axiome 5).

On a la propriété annoncée et on peut remarquer

qu'il n'existe pas de variété $A > P$ contenue dans tous

les plans passant par P .

c) Une variété A quelconque de $(\mathcal{L})$ peut s'exprimer comme

une intersection de plans.

Soit A la variété considérée ; appliquons la

loi faible de couverture,

$$\exists P_1, P_2, \dots, P_d \in (\mathcal{L}),$$

telles que :

$$A \not< A \cup P_1 \not< A \cup P_1 \cup P_2 \not< \dots \not< A \cup P_1 \cup P_2 \cup \dots \cup P_d = u$$

Appliquons alors l'axiome 5, on en déduit :

$$\exists H_1, H_2, \dots, H_d \in (\mathcal{L}),$$

telles que :

$$u \not> H_1 \not> H_1 \cap H_2 \not> \dots \not> H_1 \cap H_2 \cap \dots \cap H_d = A$$

D'où la propriété annoncée : $A = \bigcup_{H_i} H_i$ $i \in \llbracket 1, d \rrbracket$

d) Soient deux variétés quelconques A et B , telles que :

$$A \not> B. \text{ Il existe des plans } H_i \text{ de } (\mathcal{L}), \text{ tels que :}$$

$$A \not> A \cap H_1 \not> A \cap H_1 \cap H_2 \not> \dots \not> A \cap H_1 \cap \dots \cap H_n = B.$$

On vient de voir que toute variété peut s'exprimer

comme une intersection de plans. On a donc, par exemple :

$$A = \bigcup_{i \in I} H_i \quad \text{et} \quad B = \bigcup_{j \in J} H'_j$$

Chaque plan H_i contenant A contient B. Supposons par exemple l'égalité de H_i avec H'_j pour $i = j \in K$,

$K \subset J$.

Solent alors les plans H'_j restants (c'est-à-dire, tels que $j \notin K$).

Pour chacun d'eux, on a :

$$A \supset A \cap H'_j \quad \forall j \notin K, \quad j \in J.$$

Donc, il existe I, tel que :

$$A \supset A \cap H'_{j_1} \supset A \cap H'_{j_1} \cap H'_{j_2} \supset \dots \supset A \cap H'_{j_1} \cap H'_{j_2} \cap \dots \cap H'_{j_l} = A$$

$$(j_1, j_2, \dots, j_l) \in (J-K)^l$$

$$j_1 \neq j_2 \neq \dots \neq j_l.$$

La propriété annoncée est donc démontrée.

- Remarquons que lorsque l'on écrit $A = \bigcup_{i \in I} H_i$, on suppose, ce qui est possible (propriété c)) $i \in I, d]$

que :

$$H_{i_1} \supset H_{i_1} \cap H_{i_2} \supset \dots \supset H_{i_1} \cap H_{i_2} \cap \dots \cap H_{i_d}$$

$$\forall (i_1, i_2, \dots, i_d) \in I^d, \quad i_1 \neq i_2 \neq \dots \neq i_d.$$

Il est bien certain que, s'il existe H, tel que

$A \subset H$, on a aussi :

$$A = (\bigcup_{i \in I} H_i) \cap H.$$

- Si l'on utilise, d'autre part, la réciproque de la loi de couverture démontrée en a), on en déduit

l'existence de points $P_1, P_2, \dots, P_l$, tels que :

$$B \subset B \cup P_1 \subset B \cup P_1 \cup P_2 \subset \dots \subset B \cup P_1 \cup P_2 \cup \dots \cup P_l = A$$

On a ainsi formé de deux façons équivalentes, une même chaîne maximale allant de B à A.

e) Si u est union de $k+1$ points, par tout point de $(\mathcal{L})$,

il passe au moins $k+1$ plans.

Supposons que u soit union de $k+1$ points $P_1, P_2, \dots, P_{k+1}$ avec les propriétés de l'axiome 4.

Considérons alors les plans

$$H_{i_1 i_2 \dots i_k} = P_{i_1} \cup P_{i_2} \cup \dots \cup P_{i_k}$$

$$\forall (i_1, i_2, \dots, i_k) \in [1, k+1]^k,$$

$$i_1 \neq i_2 \neq \dots \neq i_k$$

Il y a $k+1$ plans $H_{i_1 i_2 \dots i_k}$ que l'on désignera pour simplifier l'écriture par $H_1, H_2, \dots, H_{k+1}$.

Vue leur construction, ces $k+1$ plans possèdent la propriété suivante :

$$H_1 \supset H_1 \cap H_2 \supset H_1 \cap H_2 \cap H_3 \supset \dots \supset H_1 \cap H_2 \cap \dots \cap H_k \supset H_1 \cap \dots \cap H_{k+1} =$$

Par le point $H_1 \cap H_2 \cap \dots \cap H_k$, il passe donc déjà k plans : les plans $H_1, H_2, \dots, H_k$. Mais il en passe au moins

un autre : c'est le plan parallèle à H_{k+1} (Postulat Euclide).

On vient de voir que par un point du treillis, il passe au moins $k+1$ plans. Par tout point du treillis, il passe donc au moins $k+1$ plans, par application du Postulat d'Euclide.

f) Soient deux variétés A et B, tels que $A \not\supset B$.

Supposons que $A = \bigcup_i P_i$, les points P_i $i \in [1, n+1]$

possédant les propriétés de l'axiome 4. Alors il existe $n+1$ points P_i , tels que :

$$A = \bigcup_i P_i, \quad B = \bigcup_{i \in [1, n+1]} P_i$$

et :

$$(\bigcup_{i \in I} P_i) \cup P_k \not\supset (\bigcup_{i \in I} P_i), \quad A \subset \{1, 2, \dots, n+1\}, \quad A \not\subset I.$$

Démonstration.

Soit $A \not\supset B$. On sait qu'il existe des plans, supposons qu'il y en ait $n+1$, $H_1, H_2, \dots, H_{n+1}$, tels que :

$$A \not\supset A \cap H_1 = B \not\supset B \cap H_2 \not\supset B \cap H_2 \cap H_3 \not\supset \dots \not\supset B \cap H_2 \cap H_3 \cap \dots \cap H_n \not\supset$$

$$O = B \cap H_2 \cap \dots \cap H_{n+1}$$

(en vertu de l'axiome 5, de la propriété b) et de la propriété e).

Solent alors les points :

$$P_1, i_2, \dots, i_n = A \cap H_1 \cap H_2 \cap \dots \cap H_{i_n}$$

$$i_1 \neq i_2 \neq \dots \neq i_n, \quad (i_1, i_2, \dots, i_n) \in [1, n+1]^n$$

Il y a $n+1$ tels points.

Nous allons voir que :

$$A = \bigcup_i P_i, \quad B = \bigcup_{i \in I} P_i, \quad A(i_1, i_2, \dots, i_n) \neq (i_2, i_3, \dots, i_n)$$

et :

$$\left(\bigcup_{i_1 i_2 \dots i_h} P_{i_1 i_2 \dots i_h} \right) \cup P_{j_1 j_2 \dots j_h} > \left(\bigcup_{i_1 i_2 \dots i_h} P_{i_1 i_2 \dots i_h} \right) \in I$$

$$I \subset \{1, 2, \dots, h+1\}$$

$$\forall (j_1, j_2, \dots, j_h) \notin I$$

La propriété annoncée sera alors établie.

Tout d'abord $P_{i_1 i_2 \dots i_h} \in A \quad \forall (i_1 i_2 \dots i_h)$,
les $h+1$ points construits appartiennent à A. De même,

$$P_{i_1 i_2 \dots i_h} \in B \quad \forall (i_1 i_2 \dots i_h) \neq (2, 3, \dots, h+1),$$

il y a donc h points appartenant à B.

De façon générale, soit $A \cap H_1 \cap H_2 \cap H_3$ pour fixer les idées.

Les points $P_{i_1 i_2 \dots i_h}$ appartiennent à $A \cap H_1 \cap H_2 \cap H_3$ pourvu que : $(i_1 i_2 \dots i_h)$ soit de la forme : $(1, 2, 3, i_4, \dots, i_h)$. Il y a donc $h-2$ points appartenant à $A \cap H_1 \cap H_2 \cap H_3$.

On a donc finalement :

$$\begin{aligned} & - h+1 \text{ points } P_{i_1 i_2 \dots i_h} \in A \\ & - h \text{ points } P_{i_1 i_2 \dots i_h} \in B = A \cap H_1 \\ & - h-1 \text{ points } P_{i_1 i_2 \dots i_h} \in A \cap H_1 \cap H_2 \end{aligned}$$

⋮

$$\begin{aligned} & - 1 \text{ point } P_{i_1 i_2 \dots i_h} \in A \cap H_1 \cap \dots \cap H_h \\ & - 0 \text{ point } P_{i_1 i_2 \dots i_h} \in A \cap H_1 \cap \dots \cap H_{h+1} \end{aligned}$$

Vue la relation :

$$A > B > A \cap H_1 \cap H_2 > \dots > A \cap H_1 \cap \dots \cap H_n > 0 ,$$

on a en particulier :

$$A = \bigcup P_{i_1 i_2 \dots i_h} \text{ et } B = \bigcup P_{i_1 i_2 \dots i_h} \\ V(i_1 i_2 \dots i_h) \neq (2, 3, \dots, h+1)$$

De façon générale, soit la variété C suivante :

$$C = A \cap H_{j_1} \cap H_{j_2} \cap \dots \cap H_{j_{h_1}} \\ h_1 \leq h .$$

$$j_1 \neq j_2 \neq \dots \neq j_{h_1} , (j_1 j_2 \dots j_{h_1}) \in [1, h+1]^{h_1}$$

Les points $P_{i_1 i_2 \dots i_h}$ appartenant à C pourvu que :

$$(i_1 i_2 \dots i_h) = (j_1 , j_2 , \dots , j_{h_1} , i_{h_1+1} , \dots , i_h)$$

D'où $h-h_1+1$ points $P_{i_1 i_2 \dots i_h}$ différents et :

$$C = \bigcup P_{i_1 i_2 \dots i_h} \left\{ \begin{array}{l} A(i_{h_1+1}, \dots, i_h) \\ i_1 = j_1 \\ \vdots \\ i_{h_1} = j_{h_1} \end{array} \right.$$

Soit alors un autre point $P_{i_1 i_2 \dots i_h}$. Supposons par exemple que ce point appartienne aux plans $H_{j_1} , H_{j_2} , \dots , H_{j_{h_1-1}}$ sans appartenir à $H_{j_{h_1}}$.

Autrement dit :

$$P_{i_1 i_2 \dots i_h} = A \cap H_1 \cap H_2 \cap \dots \cap H_{j_{h_1-1}} \cap H_{j_{h_1+1}} \cap \dots \cap H_{h+1}$$

On a :

$$A \cap H_{j_1} \cap \dots \cap H_{j_{h_1-1}} < C = A \cap H_{j_1} \cap H_{j_2} \cap \dots \cap H_{j_{h_1}}$$

Or le point $P_{i_1 i_2 \dots i_h}$ précédent appartient

$$\text{à } A \cap H_{j_1} \cap \dots \cap H_{j_{h_1-1}} \text{ sans appartenir à } C. \text{ Donc :}$$

$$C \cup P_{i_1 i_2 \dots i_h} > C.$$

$$c. q. f. d.$$

e) En utilisant f), on voit qu'à toute variété A, on

peut attacher une dimension $d(A)$ égale au nombre diminué d'une unité de points définissant A et une hauteur $h(A)$ égale à $d(A)+1$.

Ceci est valable pour l'élément universel U

et si U est défini par $k+1$ points, on dira que le treillis $(\mathcal{K})$ est de dimension k et on le notera $(\mathcal{K})_k$.

D'autre part, on a démontré en particulier en f) que si :

$$A = \bigcup P_i \quad \text{et } B = \bigcup P'_i \quad \text{avec } A > B$$

$$i \in [1, d+1] \quad i \in [1, d'+1]$$

$$\text{on a : } d = d'+1.$$

En utilisant la propriété d), on en déduit que les treillis $(\mathcal{K})$ satisfont à la condition de Jordan-Dedekind :

Les chaînes maximales joignant deux variétés quelconques ont même longueur.

h) Parallélisme dans un treillis ($\mathcal{L}$).

La définition du parallélisme donnée dans un treillis géométrique était, rappelons-le, la suivante :

$$A \parallel B \iff \begin{cases} A \cap B = 0 \\ A \cup B > A \end{cases}$$

Cette définition ne peut plus s'appliquer dans un treillis ($\mathcal{L}$) où la loi de couverture n'est pas vérifiée. Nous prendrons la définition suivante :

$$A \parallel A' \iff A = \bigcap_{i \in I} H_i, \quad A' = \bigcap_{i \in J} H'_i,$$

$$I \subset J, \quad H_i \cap H'_i = 0, \quad \forall i \in I.$$

A et A' seront donc parallèles si et seulement si :

$$A = \bigcap_{i \in I} H_i, \quad A' = \bigcap_{i \in I} H'_i, \quad \text{avec } H_i \cap H'_i = 0, \quad \forall i \in I.$$

Il est alors facile de généraliser le Postulat d'Euclide en tenant compte de cette définition.

Soit une variété A et un point P non contenus dans A. Il existe une variété A' et une seule, telle que A et A' soient parallèles.

Remarque.

La nouvelle définition du parallélisme doit coïncider avec la notion de parallélisme introduite dans Les Treillis Géométriques quand le cas se présente. Il est nécessaire pour cela d'imposer l'axiome 7, comme nous allons le voir sur un exemple simple.

Soit un treillis ($\mathcal{L}$) et soit un plan H de ce treillis.

Soit H_1 un plan non parallèle à H et soit $A = H \cap H_1$.
 Soit H_2 un plan coupant A . S'il pouvait se faire qu'un
 plan H'_2 parallèle à H_2 coupe H_1 et H sans couper A ,
 Il existerait alors dans H , par tout point de $H \cap H_1 \cap H_2$,
 deux variétés parallèles à $H'_2 \cap H$: A et $H_2 \cap H$.

Le Postulat d'Euclide ne pourrait plus être
 généralisé aux variétés à moins de donner une définition
 du parallélisme ne coïncidant pas avec celle des Treillis
 Géométriques, ce que nous éviterons donc moyennant l'axiome 7.

i) Les treillis $(\mathcal{L})$ sont complémentés.

Démonstration.

Soit A une variété d'un treillis $(\mathcal{L})$, telle que :

$$A = H_1 \cap H_2 \cap \dots \cap H_d$$

A étant de dimension $k-d$.

On sait qu'il existe $k-d$ plans, H_{d+1} , ..., H_k , tels
 que :

$$A > A \cap H_{d+1} > A \cap H_{d+1} \cap H_{d+2} > \dots > A \cap H_{d+1} \cap \dots \cap H_k$$

On définit ainsi un point P comme l'intersection
 des k plans H_i et on sait qu'il existe au moins un plan
 supplémentaire ne passant pas par P et n'étant pas paral-
 lèle aux plans précédents.

Soit H_{k+1} l'un de ces plans.

Considérons alors les points :

$$\alpha) P_{i_1 i_2 \dots i_k} = H_1 \cap H_2 \cap \dots \cap H_d \cap H_{i_{d+1}} \cap H_{i_{d+2}} \cap \dots \cap H_{i_k}$$

$$(i_{d+1}, i_{d+2}, \dots, i_k) \in [d+1, k+1]^{k-d}, i_{d+1} \neq i_{d+2} \neq \dots \neq i_k$$

Il y a exactement $k+1-d$ tels points et ils définissent la variété A .

Ces points seront notés : $P_1, P_2, \dots, P_{k+1-d}$.

$$\beta) P_{i_1 i_2 \dots i_k} = H_{i_1} \cap H_{i_2} \cap \dots \cap H_{i_k}$$

$$(i_1 i_2 \dots i_k) \in [1, k+1]^k, i_1 \neq i_2 \neq \dots \neq i_k.$$

Il y a exactement d points différents des points précédents : ces points seront notés : $P'_1, P'_2, \dots, P'_d$.

Il est facile dès lors de constater :

$$-(P'_1 \cup P'_2 \cup \dots \cup P'_d) \cup (P_1 \cup P_2 \cup \dots \cup P_{k+1-d}) = U$$

$$-(P'_1 \cup P'_2 \cup \dots \cup P'_d) \cap (P_1 \cup P_2 \cup \dots \cup P_{k+1-d}) = 0$$

En effet, on a considéré une famille de plans dont l'intersection n'avait aucun point commun.

D'autre part,

$$P'_1 \cup P'_2 \cup \dots \cup P'_d = H_{d+1} \cap H_{d+2} \cap \dots \cap H_{k+1} = A'$$

A' étant une variété à $d-1$ dimensions.

Il est donc bien évident, vue la définition de A' (resp.^t de A) comme intersection de plans, que $A \cap A' = 0$.

Et, bien sûr, $A \cup A' = U$. On a donc exhibé un complément A' de A .

c. q. f. d.

j) Lemme 1.

$\forall A_1 \in H, \exists P \in (\mathcal{C}) \Rightarrow A_1 \cup P \succ A_1$. Alors si $P \notin H$, on a :

$$(A_1 \cup P) \cap H = A_1.$$

Démonstration.

$$A_1 \cup P \supset (A_1 \cup P) \cap H$$

(loi duale de couverture)

$$A_1 \cup P \supset A_1$$

Or :

$$A_1 < (A_1 \cup P) \cap H \quad (\text{puisque } A_1 < H)$$

D'où :

$$A_1 < (A_1 \cup P) \cap H < A_1 \cup P \quad \text{avec } A_1 < A_1 \cup P$$

Donc :

$$(A_1 \cup P) \cap H = A_1.$$

k) Lemme 2.

$$\text{Si } \forall A_1 \in H, \exists P \notin H, \exists P_1 \notin H \Rightarrow A_1 \cup P \cup P_1 \supset A_1 \cup P \supset A_1$$

$$\text{Alors : } (A_1 \cup P \cup P_1) \cap H \supset A_1.$$

Démonstration.

$$\text{On a : } A_1 \cup P \cup P_1 \supset (A_1 \cup P \cup P_1) \cap H$$

(loi duale),

$$\text{et : } A_1 \cup P \supset (A_1 \cup P) \cap H = A_1$$

(lemme 1.)

Or :

$$(A_1 \cup P \cup P_1) \cap H \supseteq (A_1 \cup P) \cap H = A_1$$

Soit h la hauteur de $A_1 \cup P \cup P_1$.

On a :

$$h \left[(A_1 \cup P \cup P_1) \cap H \right] = h \left[A_1 \cup P \cup P_1 \right] - 1 = h-1$$

Or :

$$h \left[A_1 \cup P \right] = h - 1$$

$$h \left[A_1 \right] = h-2$$

On a donc :

$$h \left[(A_1 \cup P \cup P_1) \cap H \right] = h(A_1) + 1$$

et :

$$(A_1 \cup P \cup P_1) \cap H \geq A_1$$

D'où :

$$(A_1 \cup P \cup P_1) \cap H > A_1$$

1) Théorème 1.

Tout sous-treillis de $(\mathcal{C})$ obtenu en coupant $(\mathcal{C})$ par un plan H est un treillis $(\mathcal{C})$.

Si le treillis initial était de dimension n , le second sera de dimension $n-1$.

Démonstration.

Les points du nouveau treillis seront les points du plan H . Les plans du nouveau treillis, les intersections distinctes et non vides des plans H_i du treillis initial avec H : $H \cap H_i$.

L'axiome 1 est vérifié, l'élément universel du nouveau treillis étant maintenant le plan H .

L'axiome 4 est vérifié sans démonstration.

Seuls sont à vérifier les axiomes 2, 3, 5, 6 et 7.

Axiome 2.

Appliquons le lemme 2.

Soit une variété A incluse dans H .

Supposons que les points P et P_1 , tels que :

$$A_1 < A_1 \cup P < A_1 \cup P \cup P_1,$$

n'appartiennent pas à H .

Alors on a :

$$(A_1 \cup P \cup P_1) \cap H = A_2 > A_1.$$

Appliquons la réciproque de la loi de couverture qui est valable dans le nouveau treillis puisque l'axiome 4 y est vérifié :

$$\exists P' \in H \implies A_2 = A_1 \cup P'$$

La loi faible de couverture est vérifiée.

(Géométriquement, la droite PP_1 coupe le plan H en P').

Si P appartenait à H , il n'y aurait rien à vérifier. Examinons enfin le cas où $P \notin H$ mais où $P_1 \in H$.

$$A \cup P \cup P_1 \not\leq H \quad \text{et} \quad A \cup P \cup P_1 > A.$$

On a :

$$(A \cup P \cup P_1) \cap H < A \cup P \cup P_1$$

Ce qui entraîne (en appliquant, par exemple, la condition de chaîne de Jordan-Dedekind) :

$$(A \cup P \cup P_1) \cap H > A$$

et la loi faible de couverture est encore vérifiée en appliquant la réciproque de la loi de couverture.

Finalement, l'axiome 2 est donc valable dans le nouveau treillis.

Axiome 3.

Soit A une variété de $(\mathcal{L})$ incluse dans H.

Soit H_i un plan de $(\mathcal{L})$, tel que :

$$A \cap H_i \neq 0 \quad \text{et} \quad A \not\subseteq H_i.$$

On a :

$$A \succ A \cap H_i \quad (\text{loi duale dans le treillis initial}).$$

Mais :

$$A \cap H_i = A \cap H_i \cap H$$

Donc :

$$A \succ A \cap (H_i \cap H)$$

expression de la loi duale dans le nouveau treillis.

Axiome 5.

On sait que :

$$\forall A \succ B \quad \exists H_i \implies B = A \cap H_i$$

Supposons que :

$$B \prec A \prec H$$

On a alors :

$$A \cap H_i \cap H = A \cap H_i$$

Donc :

$$B = A \cap (H_i \cap H)$$

expression de la réciproque de la loi duale dans le nouveau treillis.

Axiome 6.

Soit H_1 un plan coupant H . On a donc : $H_1 \succ H_1 \cap H$
et $A = H_1 \cap H$ est un plan du nouveau treillis.

Soit P un point de H n'appartenant pas à A
et soit H'_1 le plan passant par P et parallèle à H_1 .
(Ce plan existe et est unique d'après l'axiome 6 dans
le treillis initial).

Alors $H'_1 \cap H$ est un plan du nouveau treillis
passant par P et parallèle à $A = H_1 \cap H$.

Supposons par l'absurde l'existence dans H
d'un autre plan $H_2 \cap H$ passant par P et parallèle à A .
On doit donc avoir :

$$H_1 \cap H \cap H_2 \cap H = H_1 \cap H_2 \cap H = 0.$$

Soit la variété : $B = H_2 \cap H$.

On a :

$$B \succ B \cap H'_1$$

et on a :

$$H'_1 \cap H_1 = 0$$

Donc :

$$B \succ B \cap H_1 \text{ (axiome 7 dans le treillis initial)}$$

mais :

$$B = H_2 \cap H$$

Donc :

$$H_2 \cap H_1 \cap H \neq 0$$

On aboutit à une contradiction. C'est que l'hypothèse de départ était absurde, et finalement, le Postulat d'Euclide est vérifié dans le nouveau treillis.

Axiome 7.

Soient H_1 et H_2 deux plans du nouveau treillis, tels que : $H_1 \cap H_2 = 0$.

Soit A une variété de H , telle que : $A \succ A \cap H_1$.
Supposons alors par l'absurde que :

$$H_2 \cap A = 0.$$

Dans le treillis initial, il existe deux plans $\mathcal{H}_1$ et $\mathcal{H}_2$, tels que :

$$H_2 = \mathcal{H}_2 \cap H \quad \text{et} \quad H_1 = \mathcal{H}_1 \cap H$$

et tels que :

$$\mathcal{H}_1 \cap \mathcal{H}_2 = 0.$$

Or on a :

$$A \succ A \cap \mathcal{H}_1$$

puisque :

$$\mathcal{H}_1 \cap \mathcal{H}_2 = 0$$

Cela entraîne que : $A \succ A \cap \mathcal{H}_2$ (axiome 7 dans le treillis initial).

$$\text{Mais : } A = A \cap H.$$

$$\text{Donc : } A \cap \mathcal{H}_2 = A \cap H \cap \mathcal{H}_2 = A \cap H_2$$

$$\text{Donc : } A \succ A \cap H_2$$

$$\text{et : } A \cap H_2 \neq 0.$$

On aboutit donc à une contradiction et l'axiome 7 est finalement vérifié dans le nouveau treillis).

m) Corollaire 1.

Tout sous-treillis de $(\mathcal{L})$ obtenu en coupant chaque variété de $(\mathcal{L})$ par des plans $H_1, H_2, \dots, H_h$,

non parallèles deux à deux , est un treillis $(\mathcal{L})$.

Si le treillis initial était un treillis $(\mathcal{L})_n$,
le treillis final sera un treillis $(\mathcal{L})_{n-i}$, $i \in [1, h]$.

Il suffit de réitérer h fois la démarche de 1),
pour que ce résultat soit établi.

n) Corollaire 2.

Tout sous-treillis $[0, A]$ d'un treillis $(\mathcal{L})$
est également un treillis $(\mathcal{L})$.

Il suffit de remarquer que toute variété A
d'un treillis $(\mathcal{L})$ peut être considérée comme une inter-
section de plans pour que ce corollaire découle immédia-
tement du corollaire précédent.

o) Les treillis $(\mathcal{L})$ sont relativement complémentés.

Démonstration.

Soit $A < X < B$

On doit savoir construire au moins une variété X' , telle
que :

$$\begin{cases} X \cup X' = B \\ X \cap X' = A \end{cases}$$

$[0, A]$ étant aussi un treillis $(\mathcal{L})$, il suffit de démontrer :

$$A < X < \bigcup \exists X' ,$$

tel que :

$$\begin{cases} X \cup X' = U \\ X \cap X' = A \end{cases}$$

Supposons que X soit de dimension $k-d$, alors que A est
de dimension $k-d_1$, $d_1 > d$.

On peut écrire alors :

$$X = H_1 \cap H_2 \cap \dots \cap H_d$$

$H_1, H_2, \dots, H_d$ étant d plans de $(\mathcal{C})$. De même :

$$A = X \cap H'_1 \cap H'_2 \cap \dots \cap H'_{d_1-d}$$

$H'_1, H'_2, \dots, H'_{d_1-d}$ étant d_1-d plans de $(\mathcal{C})$.

On connaît alors l'existence de $k-d_1+1$ plans de $(\mathcal{C})$:

$$H''_1, H''_2, \dots, H''_{k-d_1+1}$$

ayant avec les plans précédents la propriété énoncée en 2) e).

Dès lors, soient les familles de points suivantes :

$$\alpha) P_{i_1 i_2 \dots i_k} = A \cap \left[H''_{i_1} \cap H''_{i_2} \cap \dots \cap H''_{i_{k-d_1}} \right]$$

$$(i_1, i_2, \dots, i_{k-d_1}) \in [1, k-d_1+1]^{k-d_1}, \quad i_1 \neq i_2 \neq \dots \neq i_{k-d_1}$$

On construit ainsi $k-d_1+1$ points différents, soient $P_1, P_2, \dots, P_{k-d_1+1}$, et on a :

$$A = P_1 \cup P_2 \cup \dots \cup P_{k-d_1+1}$$

avec, pour ces points, les propriétés de l'axiome 4.

$$\beta) P_{i_1 i_2 \dots i_k} = X \cap \left[\bigcap_{i \in [1, k-d_1+1]} H''_i \right] \cap \left[H'_{i_1} \cap H'_{i_2} \cap \dots \cap H'_{i_{d_1-d-1}} \right]$$

$$(i_1, i_2, \dots, i_{d_1-d-1}) \in [1, d_1-d]^{d_1-d-1},$$

$$i_1 \neq i_2 \neq \dots \neq i_{d_1-d-1}$$

On construit ainsi d_1-d points différents, soient :

$P'_1, P'_2, \dots, P'_{d_1-d}$ et on a :

$$X = A \cup P'_1 \cup P'_2 \cup \dots \cup P'_{d_1-d} =$$

$$(P_1 \cup P_2 \cup \dots \cup P_{k-d_1+1}) \cup (P'_1 \cup P'_2 \cup \dots \cup P'_{d_1-d})$$

avec, pour ces points, les propriétés de l'axiome 4.

$$\gamma) P_{i_1 i_2 \dots i_k} = \left(\bigcap_{i \in [1, d_1-d]} H'_{i_1} \right) \cap \left(\bigcap_{i \in [1, k-d_1+1]} H''_{i_1} \right) \cap (H_{i_1} \cap H_{i_2} \cap \dots \cap H_{i_{d-1}})$$

$$(i_1 i_2 \dots i_{d-1}) \in [1, d]^{d-1}, i_1 \neq i_2 \neq \dots \neq i_{d-1}$$

On construit ainsi d points différents, soient :

$P''_1, P''_2, \dots, P''_d$.

Soit alors X' la variété suivante :

$$X' = A \cup P''_1 \cup P''_2 \cup \dots \cup P''_d$$

$$= P_1 \cup P_2 \cup \dots \cup P_{k-d_1+1} \cup P''_1 \cup P''_2 \cup \dots \cup P''_d$$

avec, pour ces points, les propriétés de l'axiome 4.

Il est facile de constater que :

$$X \cup X' = U$$

et :

$$X \cap X' = A$$

On a donc construit un complément relatif pour X ,
soit X' .

c. q. f. d.

3) - Equivalence des treillis $(\mathcal{C})$ avec les réseaux (R) .

a) Théorème 2.

L'existence d'un treillis $(\mathcal{L})$ implique l'existence d'un réseau (R) .

Démonstration.

La démonstration se fera par récurrence. Considérons tout d'abord les treillis $(\mathcal{L})$ de dimension 2.

Treillis $(\mathcal{L})_2$.

Ces treillis ne comprennent que des points et des droites (variétés de dimension 1).

Si deux droites ne sont pas parallèles, elles se coupent en un point et un seul (loi duale affaiblie).

D'autre part, la relation de parallélisme est une relation d'équivalence.

Soient $F_1, F_2, \dots, F_N$ les classes de droites parallèles. Soit P un point quelconque du treillis. Par P , il passe une droite et une seule de chaque classe (Postulat d'Euclide).

On reconnaît là les axiomes de définition d'un réseau plan (R) : rappelons en effet que la donnée d'un système : $(E, F, F_i, i \in [1, N], R, q, 2)$ vérifiant :

$$(1) \forall x \in E, \forall i \in [1, N], \text{Card} [y : y \in F_i, (x, y) \in R] = 1$$

$$(2) \forall (i, j) \in [1, k]^2, i \neq j, \forall (y, y') \in F_i \times F_j :$$

$$\text{Card} [x ; x \in E, (x, y) \in R, (x, y') \in R] = 1,$$

définit un réseau plan (R) .

Le théorème proposé est donc vérifié pour $n = 2$.

Treillis $(\mathcal{C})_n$.

Supposons qu'aux treillis $(\mathcal{K})$ de dimension $(n-1)$ correspondent des réseaux (R) de dimension $n-1$. Soit alors un treillis $(\mathcal{K})$ de dimension n .

Il s'agit de démontrer qu'il lui correspond un réseau (R) de dimension n et le théorème proposé sera établi par récurrence.

On a vu que tout sous-treillis $[0, A]$ de $(\mathcal{K})$ est un treillis possédant les mêmes propriétés que $(\mathcal{K})$; donc, à tout sous-treillis de $(\mathcal{K})$ de dimension $n-1$, obtenu en coupant les variétés de $(\mathcal{K})$ par un plan H , correspond un réseau (R) de dimension $n-1$.

Soient deux tels réseaux (R) :

$$[E, F, F_j, j \in [1, N], R, q_i, n-1]$$

et

$$[E', F', F'_j, j \in [1, N], R', q'_i, n-1]$$

obtenus à partir de deux plans H_1 et H_2 non parallèles de $(\mathcal{K})$.

Il y a donc $q_i - 1$ plans parallèles à H_2 et $q'_i - 1$ plans parallèles à H_1 .

Mais on aurait alors pour le nombre N de points du treillis $(\mathcal{K})_n$:

$$- \text{ soit : } q_i (q'_i)^{n-1}$$

$$- \text{ soit : } q'_i (q_i)^{n-1}$$

On doit donc avoir :

$$q_i (q'_i)^{n-1} = q'_i (q_i)^{n-1}$$

Ce qui entraîne :

$$q_i = q'_i = q$$

Autrement dit, les réseaux (R) de dimension $n-1$ issus du treillis $(\mathcal{L})_n$ ont chacun des classes de q plans parallèles, q étant un certain nombre entier attaché au treillis $(\mathcal{L})_n$.

Au treillis $(\mathcal{L})_n$ correspond enfin un réseau (R) de dimension n de la façon suivante :

- Les points de ce réseau sont les points du treillis.
- Les plans de ce réseau sont les plans du treillis.

Le postulat d'Euclide implique que par tout point, il passe un plan et un seul de chaque classe.

Il est facile de vérifier enfin, d'autre part, que les intersections de plans ont les propriétés voulues.

Ainsi, par exemple, deux plans du treillis $(\mathcal{L})_n$ se coupent suivant q^{n-2} points. En effet, cela revient à compter le nombre ^{de points} d'un plan d'un réseau (R) de dimension $n-1$ issu du treillis $(\mathcal{L})_n$.

b) Théorème 3.

L'existence d'un réseau (R) implique l'existence d'un treillis $(\mathcal{L})$.

Démonstration.

Soit un réseau (R) . Si ce réseau (R) peut être considéré comme un treillis, les éléments (ou variétés) de ce treillis seront définis comme des intersections

de plans du réseau (R).

$A \cap B$ représentera les points communs à A et B.

$A \cup B$, la plus petite variété contenant A et B.
Cette variété existe et est unique.

En effet, pour :

$$A = \bigcap_{i \in I} H_i$$

$$B = \bigcap_{j \in J} H_j ,$$

On a :

$$A \cup B = \bigcap_{i \in I \cup J} H_i$$

(A remarquer que dans cette notation, on définit A et B comme les intersections de tous les plans du réseau passant par A ou par B).

On a donc bien finalement un treillis dont l'élément nul est l'ensemble vide (de points) et l'élément universel, l'ensemble E des points du réseau (R).

Il reste à vérifier que ce treillis $(\mathcal{C})$ est un treillis $(\mathcal{C})_n$, c'est-à-dire, à vérifier les axiomes 2, 3, 4, 5, 6, 7 de définition des treillis $(\mathcal{C})_n$.

La vérification des axiomes 3, 5, 6 et 7 est immédiate.

Les seuls axiomes à vérifier pour que ces treillis soient des treillis $(\mathcal{C})$ sont donc les axiomes 2 et 4.

$$\text{Si } A = H_1 \cap H_2 \cap \dots \cap H_k$$

$$\text{et } A_1 = H_1 \cap H_2 \cap \dots \cap H_{k-1}$$

avec $A_1 \not\subset H_k$

On a : $A_1 > A$,

il suffit alors de prendre un point P dans H_k et non dans A pour que :

$$A \cup P > A. \quad (A_1 = A \cup P)$$

Le procédé de démonstration de l'axiome 4 est analogue.

c) Il y a donc équivalence entre treillis de dimension n $(\mathcal{L})_n$ et réseau de dimension n .

IV. Treillis associé à un système de Plans.

1) - Théorème 1.

L'existence d'une géométrie projective affaiblie entraîne l'existence d'un système de Plans (S).

Démonstration.

Les points du Système de Plans sont les points de la géométrie. Les plans de (S), les plans de la géométrie.

A une variété $A = P_1 \cup P_2 \cup \dots \cup P_h$ du treillis correspond la variété v de (S) caractérisée par les points $P_1, P_2, \dots, P_h$, la notion d'indépendance dans le treillis impliquant facilement la notion d'indépendance dans le système de plans (S).

Les propriétés des plans dans (S) sont alors faciles à établir.

2) - Théorème 2.

L'existence d'un Système de Plans (S) implique

l'existence d'une géométrie projective affaiblie.

Démonstration.

Il s'agit de démontrer les 3 axiomes de définition d'un treillis géométrique et l'axiome 4 a supplémentaire pour caractériser une géométrie projective affaiblie.

Montrons tout d'abord comment on peut associer un treillis à un système de Plans.

A chaque point du système de Plans, on fait correspondre un point du treillis cherché ($\mathcal{L}$).

A chaque plan du système de Plans, on fait correspondre un plan de ($\mathcal{L}$).

A chaque variété du système de Plans, on fait correspondre une variété de ($\mathcal{L}$).

A l'ensemble vide (de points) du système de Plans, on fait correspondre l'élément nul de ($\mathcal{L}$) et à l'ensemble E du système de Plans, on associe enfin l'élément universel U de ($\mathcal{L}$).

On a ainsi obtenu un treillis à élément nul et élément universel : effectivement, soient deux variétés quelconques V_i et V_j .

$V_i \cap V_j$ représente l'ensemble des points communs à V_i et à V_j , c'est-à-dire, la plus grande variété incluse dans V_i et V_j .

De même $V_i \cup V_j$ représente l'ensemble des points de la plus petite variété contenant V_i et V_j .

Il est facile de s'assurer, vues les propriétés des Systèmes de Plans, que $V_i \cap V_j$ et $V_i \cup V_j$ existent et sont uniques.

Rappelons, d'autre part, que dans un système de Plans, étant donnée une variété V et un point x non contenu dans cette dernière, V et x caractérisent une variété V_1 de dimension $h+1$ si V était de dimension h . Autrement dit, pour $(\mathcal{C})$: $V \cup x \succ V$.

D'où l'axiome 2 des Treillis Géométriques.

Une variété étant caractérisée par ses points indépendants, l'axiome 3 en découle immédiatement.

Il ne reste plus qu'à contrôler la loi duale affaiblie (axiome 4 a). Vue la définition des variétés comme intersection de certains plans, cette loi est immédiatement vérifiée.

En effet, soit :

$$V = \bigcap H_i$$

et soit un plan H , tel que :

$$V \not\subset H, V \cap H \neq 0.$$

On a donc :

$$\text{Card} [\bigcap H_i] \succ \text{Card} [(\bigcap H_i) \cap H]$$

$(\bigcap H_i) \cap H$ définit une variété V' , telle que :

$$V \succ V'.$$

D'où l'axiome 4 a.

3) - Corollaire 1.

Il y a équivalence entre un système de plans (S) et une géométrie projective affaiblie. Si le premier est de dimension k , le second est de même dimension et réciproquement.

4) - Construction de Systèmes de Plans (S).

Nous avons déjà signalé une construction de géométrie projective affaiblie extraite d'une géométrie projective irréductible : il suffisait d'oter de cette dernière une variété et de rajouter l'élément nul.

Cette construction permet donc d'obtenir des Systèmes de Plans.

Rappelons qu'elle n'était possible que parce que la géométrie projective était irréductible.

Dans ce cas, en effet, ces géométries possèdent des propriétés supplémentaires importantes :

- deux points quelconques sont toujours perspectifs, c'est-à-dire que si ils sont distincts, la droite qui les joint contient toujours un troisième point.

- La condition de Fano est donc réalisée : toute droite contient au moins trois points. (réf. [1] page 296).

- Soient A et B deux variétés, telles que : $A \not\subset B$. La variété A est l'union de points indépendants non situés dans B. (réf. [1] page 297).

En otant, par conséquent, une variété, les variétés restantes sont toujours des unions de points : ainsi, une droite aura toujours au moins deux points.

La géométrie projective affaiblie ainsi construite est particulière : c'est en fait une géométrie affine généralisée, c'est-à-dire, une géométrie projective affaiblie vérifiant le Postulat d'Euclide généralisé (Par un point, il passe au plus une droite parallèle à une droite donnée).

- Les géométries obtenues à partir de géométries projectives quelconques, en otant une variété et en rajoutant l'élément nul, ne conviendrait que si toutes les

variétés construites étaient encore des unions de points. Il faudrait pour cela que la variété otée ne rencontre pas les points non perspectifs. Or cela est impossible, la relation pour deux points d'être perspectifs étant une relation d'équivalence ; on est donc ramené au cas de géométries projectives irréductibles.

En résumé les seuls exemples de Systèmes de Plans que nous puissions construire à partir des géométries, seront ceux issus de géométries projectives irréductibles par le procédé indiqué.

REFERENCES.

- [1] - Dubreil-Jacotin, Lesieur, Croisot. Leçons sur la théorie des treillis, des structures algébriques ordonnées et des treillis géométriques. Cahiers Scientifiques. Gauthier-Villars, 1953.

- [2] - Lecointe P. Etude d'une certaine classe de treillis en vue de la construction de plans d'expériences et de codes correcteurs d'erreurs. C. R. Acad. Sc. Paris. t 226. 17 juin 1968, p. 1206-1209.

TABLE DES MATIERES

	<u>Pages</u>
Introduction	1
<u>Chapitre I</u> : Généralisation de la notion de Réseaux Géométriques	4
I - Définition des réseaux (R)	4
II - Définition des arrangements (T_k) et application aux réseaux (R).	18
<u>Chapitre II</u> : Application des Réseaux à la construction de Codes correcteurs d'erreurs et de plans d'expériences	34
I - Application aux Codes Correcteurs d'Erreurs	34
II - Application des réseaux à la construction de plans en blocs incomplets.....	39
III - Application des réseaux à la construction de plans en blocs incomplets (suite). Le cas des tableaux orthogonaux	49
IV - Application à la construction des ovales	52

TABLE DES MATIERES
(suite)

	<u>Pages</u>
<u>Chapitre III</u> : Construction de Réseaux (R) ..	54
I - Construction de réseaux $(R)_{k-1}$ par produit direct	54
II - Généralisation de la notion de transversales	60
III - Construction d'arrangements (T_k) idempotents et d'arrangements (T_k) isotopes	78
IV - Exemples de Construction de Réseaux (R)	102
V - Exemples de constructions de Réseaux (R) dans le cas des Corps de Galois	106
 <u>Chapitre IV</u> : Réseaux Cycliques et Codes Cycliques	120
I - Introduction	120
II - Définition des Réseaux Cycliques et des Codes Cycliques	120
III - Etude algébrique des réseaux cycliques quand $X = GF(q)$	126
Annexe	151
 <u>Chapitre V</u> : Systèmes de Plans et Réseaux Associés	152

TABLE DES MATIERES
(suite)

	<u>Pages</u>
I - Introduction	152
II - Systèmes de Droites	152
III - Systèmes de Plans	156
IV - Réseaux associés à l'étude des réseaux (R)	178
 <u>Chapitre VI</u> 4 Treillis associés à des réseaux (R) et des Systèmes de Plans (S_k)	202
I - Introduction	202
II - Rappels algébriques	202
III - Treillis associé à un réseau (R)	211
IV - Treillis associé à un Système de Plans	240

DEUXIÈME THÈSE

Propositions données par la Faculté

LA THEORIE ERGODIQUE

Vu et approuvé

Paris, le ..25.. mai 1970.

Le Doyen de la Faculté des Sciences
de Paris

M. ZAMANSKY

Vu
et permis d'imprimer

Le Recteur de l'Académie de Paris

R. MALLET

